FACULTAD DE DERECHO

MASTER DE ACCESO A LA PROFESIÓN DE ABOGADO

TRABAJO FIN DE MASTER

"Los delitos informáticos contra los bienes jurídico-patrimoniales"

Autor:

José Laserna Sierra

Tutor:

Esteban Mestre Delgado

Fecha

2019

FACULTAD DE DERECHO

MASTER DE ACCESO A LA PROFESIÓN DE ABOGADO

TRABAJO FIN DE MASTER

"Los delitos informáticos contra los bienes jurídico patrimoniales"

Autor: José Laserna Sierra

Tutor: Esteban Mestre Delgado

Tribunal de Calificación:

Presidente: _____

Vocal 1º: _____

Vocal 2º: _____

Vocal 3º: _____

Calificación: _____

Fecha: _____

A mis padres, las mejores personas

que conozco y sin las cuales nada

de esto hubiera sido posible.

Resumen:

No escapará a nadie la notoria incidencia y el arraigo adquirido por los sistemas informáticos en la actualidad. Debido a ello, la delincuencia informática gana día a día más terreno frente a la delincuencia tradicional, viéndose ello influenciado por factores como la rápida evolución de la tecnología, el anonimato en la red, la generalización del uso de las nuevas tecnologías por el conjunto de la población, la reducida inversión requerida para la realización de estas conductas, así como la ausencia de fronteras en la comisión de estos delitos. Se hace así en el presente trabajo, para una mejor exposición del tema objeto del mismo, un análisis del marco general de estudio, la delincuencia informática en general, siendo para ello ciertamente constructivo, en atención a la dimensión global alcanzable por este tipo de delincuencia, la realización de un estudio comparativo sobre el tratamiento de los delitos informáticos en la legislación de países de nuestro entorno.

No se centrará sin embargo el presente trabajo en un examen exhaustivo del marco general de estudio expuesto con anterioridad, puesto que el objeto principal del mismo radica en el análisis de la delincuencia informática que atenta contra los bienes jurídicos patrimoniales, así como de la legislación española encargada de su punición, ello debido a la predominancia de los delitos informáticos contra el patrimonio frente al resto de figuras de la delincuencia informática, siendo en concreto analizadas en profundidad las figuras de estafa informática, defraudaciones de energía y análogas, los daños informáticos, y los delitos contra la propiedad intelectual.

Palabras clave:

Delitos informáticos. Internet. Patrimonio. Sistemas informáticos. Telecomunicaciones.

Abstract:

There will not escape anyone the notorious incidence and entrenched acquired by computer systems nowadays, computer crime, day by day gains more ground against traditional crime, being seen it influenced by factors as the rapid evolution of the technology, anonymity in the network, the generalization of the use of new technologies by the population as a whole, the reduced investment required to carry out these behaviors, as well as the absence of borders in the commission of these crimes. This is done in the present work, for a better exposition of the subject matter of it, through an

analysis of the general framework of study, computer crime in general, being certainly constructive, in attention to the global dimension achievable by this type of crime, the performance of a comparative study on the treatment of computer crimes legislation of neighboring countries.

However, the present work will not focus on an exhaustive examination of the general framework of study described above, since its main purpose is the analysis of computer crime that attack patrimonial heritage rights, as well as the Spanish legislation in charge of its punishment, this is due to the predominance of computer crimes against the heritage compared to the other figures of computer crime, being in particular analyzed in depth the computer fraud, energy fraud and the like, computer damage , and crimes against intellectual property.

Keywords:

Computer crime. Internet. Heritage. Computer-based system. Telecommunications.

ÍNDICE

I. Introducción 10

II. Marco de estudio general: la delincuencia informática 12

1. Evolución tecnológica y su impacto en la sociedad: la sociedad de la información y las tecnologías 12

2. Delito informático: concepto, características y tipología 18

III. Regulación de los delitos informáticos en el Derecho Comparado 25

1. Estados Unidos 25

2. Canadá 26

3. Alemania 30

4. Italia 31

5. Francia 33

6. Irlanda 37

7. Reino Unido 38

IV. Marco de estudio específico: los delitos informáticos que inciden sobre el bien jurídico patrimonio 43

Sección 1ª: La estafa informática 43

1. Concepto y denominación 43

2. Evolución normativa y regulación actual 45

3. Bien jurídico protegido 48

4. Elementos de la punición 50

4.1 Ejecución 50

4.2 Autoría y participación 52

4.3 Circunstancias 52

4.4 Penalidad 53

4.5 Responsabilidad civil 55

5. La estafa informática como delito independiente del tipo básico de estafa 56

5.1 Elementos del tipo básico de estafa 57

5.2 Elementos del tipo de la estafa informática 61

5.3 Utilización ilegítima de tarjetas de crédito o débito, cheques de viaje o datos obrantes en ellos 71

6. Formulas específicas de fraude informático 73

6.1 Obtención de claves o datos de acceso y uso fraudulento de los mismos 73

6.2 Conexiones telefónicas fraudulentas 78

6.3 Fraude en las operaciones y transacciones en el comercio electrónico 78

6.4 Envió de correos electrónicos fraudulentos 79

Sección 2ª: Las defraudaciones de fluido eléctrico y análogas 80

1. Concepto y denominación 80

2. Evolución normativa y regulación actual 81

3. Bien jurídico protegido 84

4. Elementos de la punición 84

4.1 Ejecución 84

4.2 Autoría y participación 86

4.3 Circunstancias 87

4.4 Penalidad 87

4.5 Responsabilidad civil 92

5 Elementos del tipo 93

5.1 Defraudaciones de energía y análogas 93

5.2 Uso no autorizado de terminales de comunicación 94

6. Formulas específicas 95

6.1 Formulas específicas de defraudación de energía y telecomunicaciones 96

6.2 Defraudación de procesamiento computacional 96

6.3 Otras fórmulas 98

Sección 3ª: El daño informático 99

1. Concepto y denominación 99

1.1 El tipo tradicional de daños 99

1.2 Los daños informáticos 102

2. Evolución normativa y regulación actual 105

3. Bien jurídico protegido 111

4. Elementos de la punición 113

4.1 Ejecución 113

4.2 Autoría y participación 117

4.3 Circunstancias 118

4.4 Penalidad 118

4.5 Responsabilidad civil 121

5. Elementos del tipo 122

6. Formulas específicas 124

6.1 Daños sobre el hardware que afectan al sistema o al software 124

6.2 Daños sobre el hardware mediante acciones del software 125

6.3 Daños al software mediante software 125

Sección 4ª: Delitos contra la propiedad intelectual, la piratería informática 127

1. Concepto y denominación 127

2. Evolución normativa y regulación actual 129

3. Bien jurídico protegido 139

4. Elementos de la punición 149

4.1 Ejecución 149

4.2 Autoría y participación 150

4.3 Circunstancias 151

4.4 Penalidad 152

4.5 Responsabilidad civil 153

5. Elementos del tipo 153

5.1 Animo de obtención de un beneficio económico directo o indirecto 153

5.2 En perjuicio de tercero 154

5.3 Modos de acción 157

5.4 Ausencia de autorización de los titulares o cesionarios 165

Conclusiones 169

Bibliografía..... 172

Anexo de jurisprudencia consultada 179

I. Introducción

Actualmente es notorio el alto grado de desarrollo de la tecnología y las telecomunicaciones, adquiriendo éstas un cierto carácter trascendental para el desarrollo de la sociedad y su funcionamiento normal. Pensemos, en aras de ejemplificar, en una caída del sistema informático del servicio público de salud por varios días o la caída del sistema informático de una planta nuclear; las consecuencias serían obviamente notorias. No está exenta de esta dependencia la esfera individual de la vida de los ciudadanos; así, por ejemplo, puede esta apreciarse en la expansión que han sufrido los dispositivos móviles como teléfonos inteligentes o *smartphones*, que permiten una conexión a la red instantánea desde prácticamente cualquier lugar y mediante los cuales se pueden realizar un sinfín de conductas, como compras a través de la red, operaciones bancarias como transferencias, consultas de saldo, subida de fotografías o comentarios a las redes sociales, entre otras muchas. En principio, tanto internet como las nuevas tecnologías parecen haber traído a la sociedad un sinfín de beneficios; sin embargo, estas no se encuentran exentas de problemática, pues es manifiesta la posibilidad de realización de comportamientos ilícitos mediante y hacia las mismas.

Surge a raíz de este fenómeno jurídico-social la idea o motivación para la realización del presente trabajo, y si bien se pretendió la realización de un estudio consistente en el análisis del conjunto de delitos informáticos recogidos por el ordenamiento penal español y la realización de un análisis más extenso de la legislación de otros países al respecto de aquella materia, debido a motivos formales de presentación, como son la extensión orientativa para los trabajos de fin de master, se decidió acotar el presente trabajo a la delincuencia informática que atañe o afecta al patrimonio en su vertiente individual. Sin embargo, ello no es óbice para la posterior consecución del estudio citado, puesto que dicha idea no sea abandonado, funcionando el presente trabajo como una introducción para la posterior realización de una tesis doctoral, como se dijo, relativa al conjunto de delitos informáticos.

Fueron así las razones que motivaron la realización del presente trabajo sobre la delincuencia informática que atenta contra el patrimonio:

- La relevancia e incidencia de estas conductas respecto al resto de delitos informáticos, configurándose las mismas, y más concretamente, la estafa informática, como los delitos informáticos por excelencia dentro de una sociedad cada vez más informatizada y dependiente de la tecnología.
- La especial incidencia social de este tipo de conductas, quedando la misma reflejada debido a las continuas y diversas manifestaciones realizadas por los medios de comunicación al respecto de estas conductas, informando o reportando continuamente a la población sobre las mismas y sobre las pautas medidas de protección adoptables contra ellas.
- La curiosidad por conocer cómo se desarrolla este tipo de conductas en la práctica, y de conocer el desarrollo legislativo, doctrinal y jurisprudencial relativo a las mismas.
- La ampliación de los conocimientos adquiridos en el Grado de Derecho y en el Master de Acceso a la Abogacía, dado que, pese a que dicha materia fue estudiada en los mismos, no pudo desarrollarse en profundidad.
- La necesidad de concreción del trabajo inicialmente previsto por un tema algo más específico por cuestiones de extensión del trabajo, en aras de adaptarlo lo máximo posible a los criterios de presentación.

Se partirá, para el estudio de la citada cuestión en el presente trabajo, de un marco general de estudio, los delitos informáticos, necesario para la contextualización del objeto principal del trabajo, donde se analizarán de forma sucinta cuestiones como el concepto de delito informático y la discusión doctrinal que suscita tal expresión, las características comunes al conjunto de delitos informáticos, unas notas de derecho comparado con la finalidad de entender cómo es la regulación de la delincuencia informática en el ordenamiento de diversos países de nuestro entorno para, posteriormente, analizar el marco de estudio específico, los delitos informáticos que atentan contra el patrimonio.

Se pretende así, dentro dicho marco especifico de estudio, realizar un análisis lo más detallado posible de la figuras relativas a la delincuencia informática recogidas por el título XIII del libro II del Código Penal, relativo a los *"delitos contra el patrimonio y contra el orden socioeconómico",* que atentan contra el patrimonio, haciendo especial énfasis a razón de su importancia, en las figuras de la estafa informática regulada por el artículo 248.2 del Código Penal, las defraudaciones de fluido eléctrico y análogas de los artículos 255 y 256 de Código Penal, el delito de daños informáticos recogido por los

artículos 264 a 264 quater del Código Penal y los delitos informáticos contra la propiedad intelectual (conocidos en este ámbito como piratería informática) regulados por los artículos 270 y siguientes del Código Penal, conceptualizando los mismos, así cono analizando su evolución normativa y regulación actual, sus elementos de la punición, elementos del tipo y algunas fórmulas específicas de comisión.

II. Marco de estudio general: la delincuencia informática

1. Evolución tecnológica y su impacto en la sociedad: la sociedad de la información y las tecnologías

A lo largo de la historia, las distintas sociedades han adquirido un alto grado de dependencia de los nuevos avances tecnológicos, evolucionando y modificando sus estructuras sociales, económicas, demográficas, culturales y políticas, en consonancia con éstos. Este impacto sobre las estructuras sociales, provocado por el nacimiento de nuevos avances tecnológicos, puede apreciarse con toda claridad durante la segunda mitad del siglo XVIII, la segunda mitad del siglo XIX y la primera del siglo XX, tras las revoluciones industriales, en la que dichos avances cambiaron, junto con otros factores, pero siendo éstos los principales, la estructuración social de la época. Así, por ejemplo, la máquina de vapor, y posteriormente, la utilización de nuevas fuentes de energía, como la electricidad y el petróleo, ocasionaron en mayor o en menor medida los primeros pasos para el cambio. Inventos como el telégrafo, la radio o el teléfono, en el ámbito de las comunicaciones, agilizaron en gran medida el proceso de globalización, así como en el ámbito del transporte lo hicieran los aviones, los automóviles, el ferrocarril o los barcos a vapor.

Desde la segunda mitad del siglo XX a la actualidad, el mayor impacto de la tecnología en la sociedad deviene principalmente del nacimiento de internet, de su alto desarrollo y del rápido avance de las nuevas tecnologías, que permiten acceso a éste. En sus orígenes, los ordenadores modernos ocupaban un espacio considerable, y fue durante los años setenta cuando comenzó a popularizarse el uso de ordenadores en el ámbito doméstico de la mano de marcas como Apple o IBM, permitiendo ya no solo a las empresas el acceso a internet, sino al resto de la población, hasta que en el año 2007, de nuevo de la mano de Apple con su primer modelo de iPhone, se generalizó el uso del

smartphone o teléfono inteligente tal y como lo conocemos hoy día, pese a que se denomine por algunos como primer *smartphone* al IBM SIMON que relativamente poco o nada tiene que ver con los terminales actuales.

Dicha generalización del uso de internet y las constantes mejoras de su infraestructura, además de otros factores como el abaratamiento y mejora de los medios de acceso a éste, han ocasionado que, a lo largo de los años, la dependencia a internet de la sociedad y de sus ciudadanos haya aumentado exponencialmente. Así, diversos autores se refieren a dicho fenómeno como la "sociedad de la información", en concreto, parece de interés referenciar a BARRANCO SAIZ[1] cuando expone con acierto que las nuevas tecnologías *"han permitido transformar los modelos tradicionales de comportamiento, desde la educación hasta la salud, pasando por el ocio o el trabajo. Todos coinciden en que las actuales políticas tecnológicas de convergencia, junto con los avances individuales en determinados campos como la telefonía móvil o la banda ancha, generan nuevos servicios de los que nos podemos beneficiar todos";* además, refleja a la perfección el grado de dependencia a la tecnología sufrido en la actualidad en cuanto expone que *"todavía más; en nuestros países, estos desarrollos que influyen directamente en el bienestar han alcanzado tal grado de «normalidad» que no son perceptibles ni somos conscientes de lo que significan para nuestra existencia, hasta que se caen, en un momento determinado, y no podemos usarlos".*

Podría decirse, así, que es tal el grado de implantación en nuestra forma de vida que ya afecta incluso al modo en el que interactuamos entre nosotros, convirtiéndose las nuevas tecnologías en un componente al parecer imprescindible en un tiempo record, habiendo reducido incluso la importancia de medios de comunicación tradicionales como el teléfono fijo, la radio o la televisión, hacia medios como las aplicaciones de mensajería instantánea, las redes sociales, servicios de entretenimiento en *streaming*, entre otras. Sin embargo, como ya se mencionó, tal dependencia no se erige únicamente a nivel individual, sino también a nivel estatal y empresarial; así, por ejemplo, es reseñable de igual forma el impacto de las nuevas tecnologías en el conjunto de administraciones públicas, debiendo destacar dado el objeto de este trabajo la influencia de dicha tecnología en la administración de justicia española, en concreto, son de apreciación tanto la exposición de motivos novena de la Ley de Enjuiciamiento Civil cuando dispone que *"la*

[1] BARRANCO SAIZ, J., *"Sociedad de la Información", Telos: Cuadernos de comunicación e innovación*, número 69, 2006, pág. 4 y 5**.**

Ley, atenta al presente y previsora del futuro, abre la puerta a la presentación de escritos y documentos y a los actos de notificación por medios electrónicos, telemáticos y otros semejantes, pero sin imponer a los justiciables y a los ciudadanos que dispongan de esos medios y sin dejar de regular las exigencias de esta comunicación", y de forma similar recoge el artículo 273 de la Ley de Enjuiciamiento Civil que *"todos los profesionales de la justicia están obligados al empleo de los sistemas telemáticos o electrónicos existentes en la Administración de Justicia para la presentación de escritos, iniciadores o no, y demás documentos, de forma tal que esté garantizada la autenticidad de la presentación y quede constancia fehaciente de la remisión y la recepción íntegras, así como de la fecha en que éstas se hicieren",* ello debido a la aprobación de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Y, si bien pareciere que tal dependencia tecnológica únicamente aportará beneficios derivados de su uso e implantación, no le resultara extraña a nadie la existencia de determinados ataques consecuencia del uso de las mismas, dado que, debido a las características de los medios tecnológicos, pueden observarse lesiones o ataques no solo a nivel individual sino también colectivo, cometidas no solo mediante medios informáticos sino también contra los mismos. Así, por ejemplo, el aumento de los delitos de pornografía infantil gracias a los modernos medios de transferencia de datos, los continuos ataques contra la intimidad, reiterados intentos de estafa informática, la incidencia en la actualidad de la piratería informática, entre otras conductas igualmente relevantes. Pueden así mencionarse, por su relevancia y a modo de ejemplo de las consecuencias negativas de tal dependencia, la crisis sufrida en el año 2017 provocada por el software malicioso tipo *ransomeware* bautizado como *WannaCry* que ha puesto en jaque la estructura de cientos de empresas (como por ejemplo, en el panorama nacional, a Telefónica) y organismos públicos de todo el mundo, llegando a desequilibrar el sistema sanitario de Reino Unido e incluso afectando al ministerio de interior ruso[2].

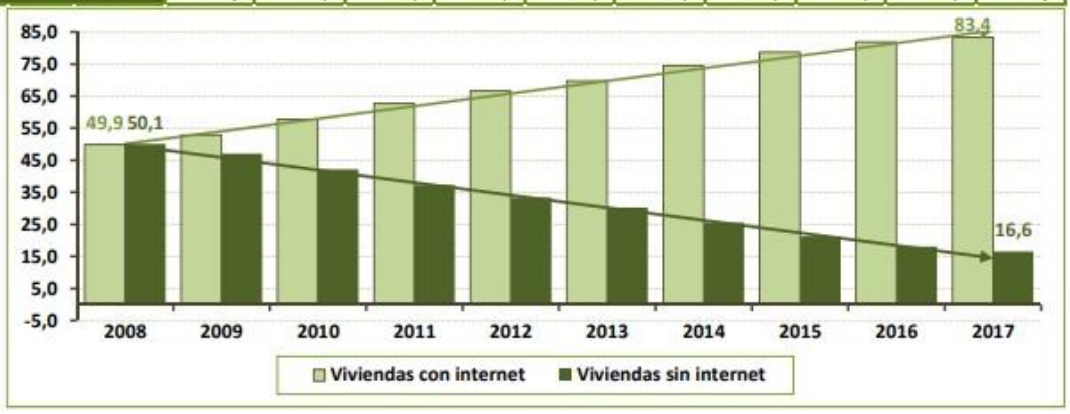
Tal es el grado de implantación de las nuevas tecnologías que diversos estudios realizados por el Ministerio del Interior conforme a los datos aportados por el INE, más concretamente, el relativo al año 2017[3], exponen datos relevantes como el porcentaje de viviendas con o sin acceso a internet, siendo en el año 2017 un 83,4% (frente al 49,9%

[2] http://www.bbc.com/mundo/noticias-39929920 (consulta 22 de mayo de 2017).
[3] http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70 (consulta 3 de enero de 2019).

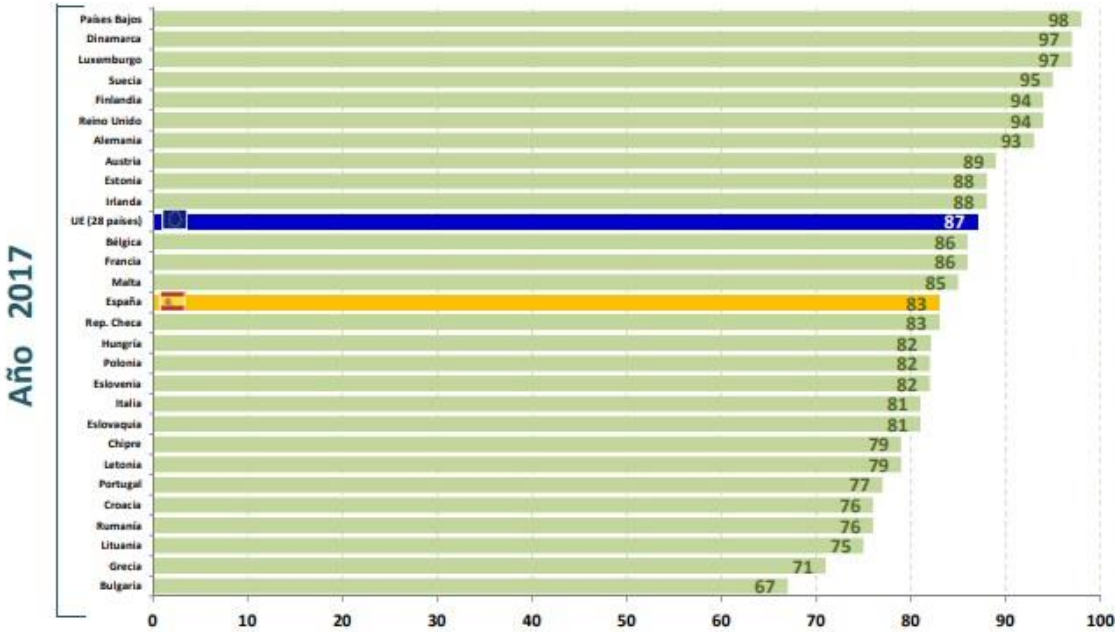
del año 2008), el porcentaje de viviendas con acceso a internet en la Unión Europea, encontrándose España por debajo de la media (87%), y el porcentaje de personas que han utilizado internet variable según el grupo de edad (43,7% los más mayores y 98% los más jóvenes).

Así pueden observarse a continuación las gráficas correspondientes a dicho estudio, en las que puede apreciarse de forma clara tanto la evolución de la implantación a internet por la población, como la dotación de la infraestructura necesaria para la conexión en el ámbito doméstico en España y en la Unión Europea:

PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET										
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Viviendas con internet	**49,9**	52,9	57,8	62,7	66,6	69,7	74,4	78,7	81,9	**83,4**
Viviendas sin internet	**50,1**	47,1	42,2	37,3	33,4	30,3	25,6	21,3	18,1	**16,6**

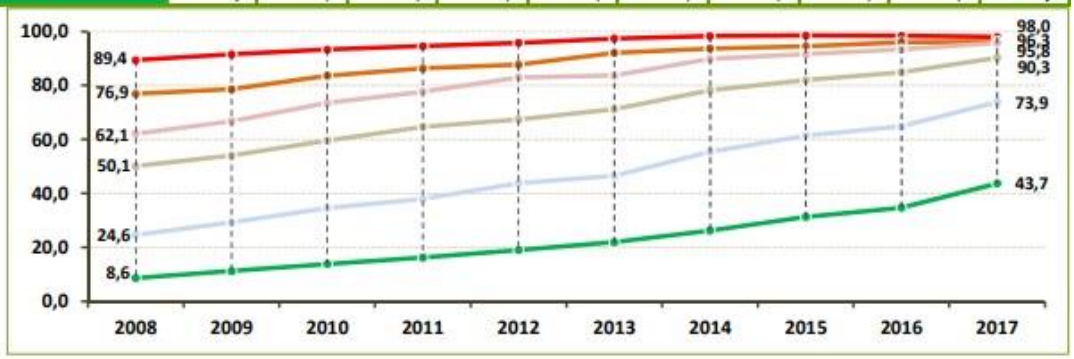


Fuente: Ministerio del Interior en "Estudio sobre la cibercriminalidad en España"



Fuente: Ministerio de Interior en "Estudio sobre la cibercriminalidad en España"

	% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES									
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Edad: De 16 a 24 años	**89,4**	91,5	93,3	94,6	95,8	97,4	98,3	98,5	98,4	**98,0**
Edad: De 25 a 34 años	**76,9**	78,6	83,6	86,3	87,7	92,1	93,7	94,5	96,0	**96,3**
Edad: De 35 a 44 años	**62,1**	66,8	73,5	77,7	83,0	83,7	89,8	91,6	93,3	**95,8**
Edad: De 45 a 54 años	**50,1**	54,0	59,6	64,6	67,4	71,2	78,2	82,0	84,9	**90,3**
Edad: De 55 a 64 años	**24,6**	29,3	34,6	37,9	43,8	46,5	55,4	61,4	64,8	**73,9**
Edad: De 65 a 74 años	**8,6**	11,2	13,8	16,2	19,0	21,9	26,2	31,3	34,7	**43,7**



Fuente: Ministerio del Interior en "Estudio sobre la cibercriminalidad en España"

Es obvio que Internet se ha erigido como un pilar fundamental para la sociedad actual y sus estructuras. Así, y al hilo de lo anterior, puede mencionarse la Resolución A/HRC/32/L.20, de la ONU, que, si bien carece de carácter vinculante, pone un especial énfasis en este medio y en la necesidad de cumplimiento de los derechos de las personas tanto dentro como fuera de éste; asimismo, merece la pena extractar parte de dicho texto en cuanto *"reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas".* Se ha de agregar a ello las diversas propuestas realizadas por la Comisión Europea, en cuanto a la reforma de la normativa relativa a las telecomunicaciones con motivo de las crecientes necesidades del conjunto de ciudadanos europeos. Se hablaba en concreto de mejoras en la conectividad en centros educativos, el acceso a la conectividad en los hogares de todos los ciudadanos europeos y la posibilidad de conexión en centros urbanos, así como en servicios de transporte para el año 2020, objetivo que parece en pleno año 2017 de difícil consecución[4]. En la misma línea, y pese a que *a priori* no exista relación aparente con la resolución ni con las propuestas de la Comisión Europea citadas con anterioridad, son muchos los municipios en España que instalan ya redes WI-FI en sus centros urbanos[5],

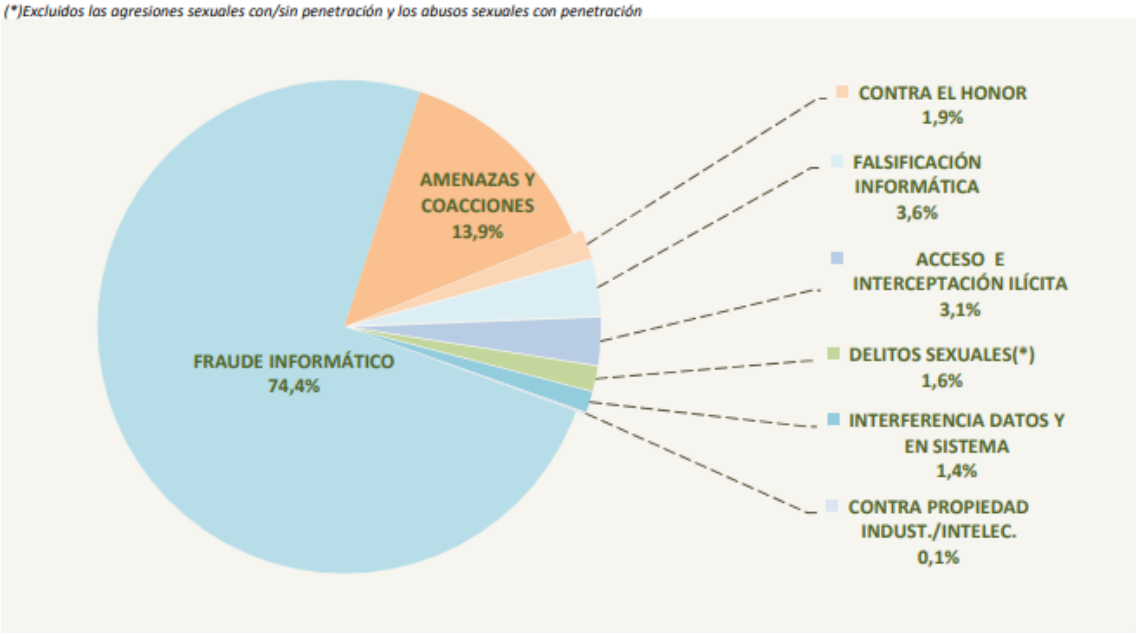
[4] http://europa.eu/rapid/press-release_IP-16-3008_en.htm (consulta 22 de mayo de 2017).
[5] http://cadenaser.com/ser/2015/02/26/ciencia/1424937716_759312.html (consulta 22 de mayo de 2017).

de manera que los ciudadanos puedan acceder de una forma rápida a internet mediante sus dispositivos[6].

En relación a los datos estadísticos aportados por el INE, y enfocándose el presente apartado en la delincuencia informática, parece relevante también la mención del estudio sobre cibercriminalidad en España, realizado por el Ministerio del Interior[7], cuando refiere mediante el siguiente grafico la evolución de la delincuencia informática desde el año 2014 al año 2017:

HECHOS CONOCIDOS	2014	2015	2016	2017
ACCESO E INTERCEPTACIÓN ILÍCITA	1.851	2.386	2.579	2.505
AMENAZAS Y COACCIONES	9.559	10.112	11.473	11.270
CONTRA EL HONOR	2.212	2.131	1.524	1.537
CONTRA PROPIEDAD INDUST./INTELEC.	183	167	121	109
DELITOS SEXUALES(*)	974	1.233	1.188	1.312
FALSIFICACIÓN INFORMÁTICA	1.874	2.361	2.697	2.961
FRAUDE INFORMÁTICO	32.842	40.864	45.894	60.511
INTERFERENCIA DATOS Y EN SISTEMA	440	900	1.110	1.102
Total HECHOS CONOCIDOS	**49.935**	**60.154**	**66.586**	**81.307**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Fuente: Ministerio del interior en "Estudio sobre la cibercriminalidad en España"

Como se desprende del gráfico expuesto con anterioridad, se aprecia un aumento exponencial de la delincuencia informática desde el año 2014 al año 2017, siendo los delitos informáticos con mayor incidencia las estafas informáticas, al abarcar un 74,4% de los casos, y las amenazas y coacciones, que abarcan un 13´9% del total de los casos.

[6] http://elpais.com/diario/2009/01/29/ciberpais/1233199465_850215.html (consulta 22 de mayo de 2017).
[7] http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf (consulta 5 de julio de 2018).

Cabe destacar, sin embargo, que dichas cifras son solo respectivas a casos conocidos, por lo que han de ser tenidas en cuenta como meros indicadores de la situación actual.

Este avance desbocado en la evolución tecnológica hace ciertamente difícil la cuestión relativa a la legislación y tipificación de las conductas que atentan contra los diversos bienes jurídicos protegidos por el Código Penal que se ven afectados en mayor o en menor medida por las conductas relacionadas con la informática y su utilización con fines delictivos. Ciertamente, se hace complicada la tarea del legislador penal en tanto cada día se desarrollan un sinfín de programas o se descubren nuevas vulnerabilidades de los sistemas informáticos; es por ello que, como se observará *infra*, el legislador, hace uso de figuras ciertamente amplias con las que se pretende abarcar un indeterminado número de conductas, permitiendo así la subsunción de las mismas en el Código Penal, en aras de evitar supuestos de lagunas de punición. Se enfrenta la actual sociedad así a un nuevo reto, el de legislar y actualizar dicha legislación en tiempos relativamente breves para acomodarse o adaptarse de una forma más precisa a la realidad o en buscar nuevos métodos para que dicha realidad no "adelante" a la legislación existente. Así, como se vio anteriormente, el legislador, en un intento, emplea un método que, si bien suscita ciertas dudas, emplea figuras de una cierta amplitud conceptual e interpretativa, que si bien, son bastante prácticas para su cometido, rozan o chocan con ciertos principios jurídico-penales, como los de legalidad y seguridad jurídica. No ha de olvidar así el legislador que la ley se dirige al ciudadano, y que el mismo ha de conocer de forma cierta y con seguridad lo que se encuentra previsto en la legislación penal, debiendo poder entender lo que se prohíbe, ordena o permite, pudiendo así guiar su actuación dentro de la legalidad.

2. Delito informático: concepto, características y tipología

Se parte en el presente epígrafe de un concepto cuanto menos difuso, puesto que, bajo tal denominación "delito informático" o "delitos informáticos" se engloban un conjunto de delitos relacionados con la informática o las tecnologías de la información y la comunicación, en adelante denominadas TIC, y que, sin embargo, no se corresponden con ninguna categoría jurídico-penal concreta, sin existir, por ende, ningún hecho punible específico que abarque tal concepto[8]. Parece así que el conjunto de autores haya adoptado

[8]Cfr. MATA Y MARTÍN, R.M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, pág. 21.

dicha terminología bien por la sencillez o simplificación con la que permite expresarse, al aunar el conjunto de conductas relacionadas con la informática o las TIC bajo dicho concepto, o bien, por una mera traducción del término anglosajón *Computer Crime* [9][10], que es aplicado de igual manera para englobar dicho conjunto de conductas relacionadas con la tecnología informática[11]. Es recalcable en este sentido, cómo un sector de la doctrina niega la aplicabilidad del término "delito informático"[12] con la finalidad de englobar estas conductas.

Se defiende en el presente trabajo la postura adoptada por GUTIERREZ FRANCES[13] y ROMEO CASABONA[14], en cuanto exponen el poco tecnicismo de la terminología "delito informático", en singular para englobar el conjunto de conductas descritas en anteriores párrafos, y en consecuencia, defendiendo de forma coherente la existencia, no de un único delito informático, sino de una pluralidad de éstos vinculados únicamente por su relación con la informática o las TIC, dado que en gran parte no comparten ni medios comisivos ni protegen los mismos bienes jurídicos. Es por ello que ambos autores aportan diversas denominaciones alternativas como "ciberdelitos", "cibercrimen", "criminalidad informática" y "delincuencia vinculada a los sistemas de procesamiento de datos". Quizá, como indica MIRÓ LLINARES, parezca más correcta la terminología "cibercriminalidad", dado que en la actualidad, con independencia del medio o plataforma informática, se cometen la mayoría de ilícitos en internet, también denominado ciberespacio[15]; en este sentido, la Real Academia Española entiende que el uso de *"Ciber-"* implica o indica *"relación con redes informáticas"*. Pese a lo anterior, e independientemente de la terminología preferida por cada autor, lo que es de manifiesto con todo lo expuesto es el continuo intento de la doctrina por realizar una agrupación de las conductas ya descritas bajo un único término que permita así referirse al conjunto de ellas.

---

[9] Cfr. GALICKI, A., *"Computer Crime", The American criminal law review,* volumen 51, número 4, 2014, pág. 1.
[10] Cfr. https://www.justice.gov/criminal-ccips (consulta 07 de junio de 2017).
[11] Cfr. GUTIERREZ FRANCES, M.L., *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pág. 49 y ss.
[12] Cfr. HERNÁNDEZ DÍAZ, L., *"El delito informático", Eguzkilore*, número 23, 2009, pág. 235.
[13] Cfr. GUTIERREZ FRANCES, M.L., *op.cit.*, pág. 51 y ss.
[14] Cfr. ROMEO CASABONA, C.M., *"De los delitos informáticos al cibercrimen",* en *Universitas vitae: homenaje a Ruperto Núñez Barbero*, Editoriales Universidad de Salamanca, Salamanca, 2007, pág. 654 y ss.
[15] Cfr. MIRÓ LLINARES, F., *"La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio", Revista Española de Investigación Criminológica*, número 11, 2013, pág. 2.

Al hilo de lo anterior, las distintas conductas que se pretenden englobar o integrar bajo la distinta terminología ya mencionada, son diferentes entre sí, bien por la protección de distintos bienes jurídicos, o bien por otros factores, y sin embargo, existen una serie de rasgos criminológicos comunes entre ellas[16], funcionando éstos como la base que permite la integración bajo una terminología concreta que se refiera al conjunto de ellos.

Se trata en primer lugar de conductas asociadas, de forma generalizada por el conjunto de la sociedad, con una delincuencia altamente tecnificada para la que requiere de conocimientos avanzados de informática en lo relativo al *software* o *hardware*; sin embargo, ello no es así, pues no debe olvidarse que en la actualidad se ha generalizado el uso del *smartphone* y la *tablet,* los cuales con un coste medio relativamente reducido, con la relativa facilidad de su utilización y mediante la posibilidad de conexión a redes inalámbricas o mediante redes móviles, mantienen un alto potencial delictivo permitiendo, por ejemplo, la utilización del correo electrónico, la transferencia de imágenes, o acceso a redes sociales, que permiten la realización de comportamientos delictivos desde prácticamente cualquier lugar[17]. Puede quizá ello deberse en mayor parte a la cultura cinematográfica que representa a los ciberdelincuentes como sujetos profesionales de la informática que utilizan pantallas verdes llenas de código binario que poco o nada tienen que ver con la realidad.

En segundo lugar, y en relación con lo expuesto en el párrafo anterior, se trata por lo general de delitos de fácil comisión y que, como se ha visto, requieren de una escasa inversión inicial en comparación al posterior perjuicio causado y lucro obtenido[18]. Así, en la actualidad, puede llegar a adquirirse un *smartphone* o *tablet* por un rango de precio aproximado de unos 100 euros en los modelos más básicos o los 1000 en modelos más avanzados. En relación al perjuicio, se caracteriza por ser de carácter elevado en líneas generales, puesto que la actuación en el medio informático se ve menos limitada que en la criminalidad clásica; así lo entiende MATA Y MARTÍN cuando expone que *"si tomamos como ejemplo el dinero, los resultados cuantitativos de la criminalidad clásica son mucho más limitados al verse constreñida a actuar sobre elementos materiales, pero*

[16] Cfr. GUTIERREZ FRANCES, M.L., *op.cit.*, págs. 71 y 72.
[17] Cfr. MIRÓ LLINARES, F., *"Cibercrimen y vida diaria en el mundo 2.0"* en *Crimen, oportunidad y vida diaria: libro homenaje al Profesor Dr. Marcus Felson*, Dykinson, Madrid, 2015, pág. 419 y ss.
[18] DE LA CUESTA ARZAMENDI, J.L., PÉREZ MACHIO, A.I., SAN JUAN GUILLEN, C., *"Aproximaciones criminológicas a la realidad de los ciberdelitos"* en *Derecho penal informático*, Civitas, Navarra, 2010, pág. 80.

sin embargo, en este caso al tratarse de dinero contable los perjuicios pueden alcanzar dimensiones mucho mayores"[19], y en el mismo sentido ROVIRA DEL CANTO cuando refiere que *"se ha venido alegando que existe otra causa , que por otro lado motiva y facilita la tendencia hacia sumas de daños cada vez más elevadas […]que el objeto del comportamiento ilícito sea el llamado dinero contable, cuya cantidad máxima no tiene por qué limitarse a la cantidad de dinero efectivo existente en caja, como sucede en los delitos clásicos económicos patrimoniales"*[20] . Por otro lado, no se limita el perjuicio a lo económico, incrementándose considerablemente también éste cuando el bien jurídico lesionado sea de carácter personal, como la intimidad o la indemnidad sexual[21]. No debemos olvidar que en el año 2014 se produjo una filtración de fotografías de índole sexual afectando a numerosos personajes públicos denominada como "*celebgate*"[22], donde puede apreciarse una magnificación del perjuicio por el propio medio, internet, que permitió la difusión a nivel global de este tipo de imágenes.

En tercer lugar, consisten por lo general en conductas dinámicas[23], es decir, en conductas caracterizadas en mayor medida por el automatismo[24] (siendo un claro ejemplo de ello la estafa informática mediante la técnica del *spam* denominada *phishing*, que se analizará en sucesivos apartados de este trabajo), permitiendo así mediante el procesamiento de datos la realización no de un único acto, sino de una pluralidad de ellos de forma continuada y automática. Se trata pues de una posibilidad de repetición de la acción mediante la introducción de instrucciones, comandos u órdenes al sistema informático que permiten esta repetición mediante una única acción del delincuente[25].

En cuarto lugar, son conductas realizables al amparo de un cierto anonimato[26]. Se refiere así puesto que, si bien existe la posibilidad de identificación del autor de las conductas, ello no es para nada sencillo en la mayoría de los casos, bien por la ausencia de una legislación eficaz para ello, o por los continuos intentos del autor de enmascarar su identidad mediante diversos métodos ajenos al objeto de este trabajo. Baste decir que

[19] MATA Y MARTÍN, R.M., *Delincuencia informática…*, pág. 26.
[20] Cfr. ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002, pág. 81.
[21] *Ibidem*, págs. 81 y 82.
[22] http://www.abc.es/tecnologia/20140907/abci-nuestra-intimidad-desnudo-internet-201409062035.html (consulta 11 de junio de 2017).
[23] Cfr. GUTIERREZ FRANCES, M.L., *op.cit*., pág. 79 y ss.
[24] MATA Y MARTÍN, R.M., *Delincuencia informática…*, págs. 22 y 23.
[25] Cfr. ROVIRA DEL CANTO, E., *op.cit.*, págs. 78 y 79.
[26] DE LA CUESTA ARZAMENDI, J.L., PÉREZ MACHIO, A.I., SAN JUAN GUILLEN, C., *op.cit*., pág. 91.

existe tal posibilidad y que ésta dificulta seriamente las labores de descubrimiento, prueba e investigación de este tipo de conductas. Manteniendo una estrecha relación con lo anteriormente desarrollado, es cuanto menos reseñable la posibilidad de ejecución a distancia de estas conductas, favorecida en gran parte por la propia naturaleza del medio en el que las mismas se desenvuelven; se posibilita así el uso de la red para actuar desde prácticamente cualquier lugar, actuando, si se desea, a miles de kilómetros de distancia del lugar donde se produzca el resultado, superando así las barreras o fronteras nacionales y ocasionando en estos casos dificultades para la determinación de la legislación aplicable[27].

Al hilo de lo anterior, las distintas conductas que se pretenden englobar o integrar bajo la distinta terminología ya mencionada, son diferentes entre sí, bien por la protección de distintos bienes jurídicos, o bien por otros factores, y sin embargo existe una serie de rasgos criminológicos comunes entre ellas, funcionando éstos como la base que permite la integración bajo una terminología concreta que se refiera al conjunto de ellos.

Son precisamente dichos rasgos comunes y la dispersión de los tipos relativos al cibercrimen en el Código Penal, lo que ha llevado a numerosos autores a intentar realizar una clasificación de los mismos. Así, por ejemplo, autores como GONZALEZ HURTADO, que entiende que *"estas conductas serían las que engloban delitos en los que los sistemas informáticos son la herramienta fundamental para la comisión del delito […] delitos en los que el sistema informático es el objeto del delito […], y delitos relacionados con el contenido, en los que los sistemas informáticos facilitan de forma sustancial la comisión de los mismos"*[28], y en el mismo sentido TELLEZ VALDES, que realiza una clasificación en la que diferencia entre delitos informáticos en los que los sistemas informáticos funcionan como un instrumento o medio (en concreto entiende que *"en esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito")* y conductas en las que los sistemas informáticos funcionan como fin u objeto (*"en esta categoría se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física"*[29]*).*

[27] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos a través de internet,* Constitutio Criminalis Carolina (CCC), Madrid, 2007, pág. 20 y ss.
[28] GONZÁLEZ HURTADO, J.A., *"Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", La Ley Penal*, número 107, 2014, pág. 2.
[29] TELLEZ VALDES, J., *Derecho informático*, McGraw-Hill, México, 2008, págs. 190 y 191.

Autores como DE LA MATA BARRANCO o HERNÁNDEZ DIAZ[30], si bien defienden igualmente la existencia de delitos informáticos en los que los medios o sistemas informáticos son medio u objeto del delito, entienden la existencia de nuevas modalidades. Como se adelantaba, entienden la existencia de delitos cometidos contra sistemas informáticos (en los que incluyen delitos de daños contra la integridad de los sistemas o datos, delitos de hurto y apropiación indebida y delitos de robo relativos a la apropiación de soportes digitales y utilización fraudulenta de equipos o sistemas de identidad digital, delitos de defraudación relativos al abuso, acceso o utilización fraudulenta de equipos informáticos y delitos de falsificación informática), delitos cometidos a través de la informática contra sistemas informáticos o informaciones digitalizadas (categoría en la que se engloban delitos de descubrimiento y revelación de secretos mediante accesos informáticos ilícitos, interceptación de comunicaciones e intrusismo informático, delitos contra el secreto de empresa o espionaje informático industrial), delitos cometidos a través de medios informáticos (entre los que entienden subsumidos en tal categoría las defraudaciones o fraudes informáticos, delitos relativos al mercado y los consumidores mediante la facilitación o prestación ilícita de servicios restringidos, falsedades personales o adopción de identidad digital falsa, delitos de difusión de contenidos lesivos para diversos intereses como la libertad sexual , el honor, el correcto funcionamiento del mercado derechos fundamentales y libertades públicas, es decir, delitos de difusión informática), y delitos contra la gestión de derechos digitales (concurriendo en tal categoría los delitos contra la propiedad intelectual o pirateo informático y delitos contra la propiedad industrial)[31].

Por otro lado, RAYÓN BALLESTEROS Y GÓMEZ HERNÁNDEZ[32], entre otros autores[33], hacen referencia a la clasificación realizada por la Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías, en la que se realiza una clasificación ciertamente pareja a la ya expuesta. Así, dispone la citada instrucción: *"el catálogo inicial*

[30] HERNÁNDEZ DÍAZ, L., *op.cit.*, pág. 240.
[31] Cfr. DE LA MATA BARRANCO, N.J, HERNANDEZ DIAZ, L., *"Los delitos vinculados a la informática en el derecho penal español"* en *Derecho penal informático*, Civitas, Navarra, 2010, págs. 161 a 197.
[32] RAYÓN BALLESTEROS, M.C., GÓMEZ HERNÁNDEZ, J.A., *"Cibercrimen: particularidades en su investigación y enjuiciamiento", Anuario Jurídico y Económico Escurialense*, Número XLVII, 2014, pág. 216.
[33] AMADEO GADEA, S., *Código Penal. Doctrina jurisprudencial,* Factum Libri Ediciones, 2015, pág. 444.

de delitos a los que se extiende el marco competencial del área de criminalidad informática, que a continuación se expone estructurado en tres categorías", siendo tales categorías, primera, *"delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs",* en la que se incluyen delitos de daños informáticos o sabotaje informático y ataques de denegación de servicios (artículo 264 y siguientes del Código Penal), delitos de acceso sin autorización a datos, programas o sistemas informáticos (artículo 197 bis del Código Penal), delitos de descubrimiento y revelación de secretos cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos (artículo 197 del Código Penal), delitos de descubrimiento y revelación de secretos de empresa cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos o electrónicos (artículo 278 del Código Penal), delitos contra los servicios de radiodifusión e interactivos (artículo 286 del Código Penal). Como segunda categoría, la de *"delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs",* es decir, donde los sistemas informáticos son un medio para la comisión del delito, entre los que se incluyen (por la Fiscalía General del Estado) delitos de estafa informática (artículo 248.2 y siguientes del Código Penal), delitos de acoso a menores de 16 años cuando se lleve a efecto a través de las TICs, conocido habitualmente como *child grooming* (artículo 183 ter del Código Penal), delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TICs (artículo 189 del Código Penal) y delitos contra la propiedad intelectual cuando se cometan utilizando las TICs (artículos 270 y siguientes del Código Penal); y, finalmente, una tercera categoría relativa a *"delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia"*, la cual, como opinión personal, no deja de ser en realidad una subcategoría englobable en la segunda, donde se encuadran delitos de falsificación documental cuando para la ejecución del delito se hubieran empleado las TICs (artículos 390 y siguientes del Código Penal), delitos de injurias y calumnias cometidos a través de las TICs (artículos 205 y siguientes del Código Penal), delitos de amenazas y coacciones cometidos a través de las TICs (artículos 169 y siguientes del Código Penal), delitos contra la integridad moral cometidos a través de las TICs (artículo 173.1 del Código Penal), delitos de apología o incitación a la discriminación, el odio y la violencia o de

negación o justificación de los delitos de genocidio cometidos a través de las TICs (artículo 510 Código Penal), o cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs, requiriéndose para los delitos recogidos en esta última categoría, la necesaria concurrencia de una especial complejidad en la investigación criminal[34].

III. Regulación de los delitos informáticos en el Derecho Comparado

Cabe exponer a modo de introducción que el conjunto de países analizados son parte firmante del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, y por ende, se encuentran sujetos a las obligaciones contraídas en el mismo. Se trata del primer tratado internacional sobre crímenes cometidos a través de internet y redes informáticas, tratando estrechamente temas como las infracciones de derechos de autor, fraude informático, pornografía infantil y violaciones de la seguridad en la red, entre otras cuestiones[35].

1. Estados Unidos

Se configura *The United States Code* como una recopilación y codificación de la ley estatutaria federal de Estados Unidos, recogiendo este documento numerosas disposiciones relativas a los delitos informáticos. Así, son de apreciación[36]:

En lo concerniente a los delitos informáticos relacionados con el *fraud o fraude* puede mencionarse dentro del *United States Code*, título 18, parte primera, capítulo 47 las secciones 1028, 1029, 1030 y 1037.

Respecto a los daños o destrucción de materiales para las telecomunicaciones propiedad de los Estados Unidos, puede mencionarse dentro del *United States Code*, título 18, parte primera, capítulo 65 la sección 1362.

Respecto a delitos informáticos relacionados con materiales obscenos, menores, material procedente de la explotación infantil y la explotación sexual de menores pueden observarse en el *United States Code*, título 18, parte primera, capítulo 71 las secciones

[34] Cfr. España. Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías.
[35] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (consulta 15 de junio de 2017).
[36] https://www.law.cornell.edu/uscode/text (consulta 15 de junio de 2017).

1462, 1465, 1466, 1466-A, en el capítulo 110 las secciones 2251, 2252, 2251-A, 2251-B y 2251-C y en el capítulo 117 la sección 2425.

En lo referente a los derechos de autor, pueden mencionarse dentro del *United States Code*, título 18, parte primera, capítulo 113 la sección 2319, en el título 17, parte primera, capítulo 5 la sección 506 y en el título 47, parte primera, capítulo 5 la sección 605.

Pese a lo expuesto con anterioridad hemos de recordar, como bien expone ROVIRA DEL CANTO, que *"en el derecho penal estadounidense, de carácter estatutario, cada Estado se dota de sus propios estatutos penales […] limitándose el Gobierno Federal, en un papel secundario, a promulgar ciertas normas penales de ámbito nacional"*[37]. En este sentido, habría de analizarse además el conjunto de normativas penales de cada Estado; sin embargo, por cuestiones de espacio esto no se analizará de una forma exhaustiva en el presente trabajo, baste con mencionar a modo de ejemplificar lo expuesto estatutos de determinados estados. Así, por ejemplo, el estatuto de Kansas recoge en su capítulo 21, artículo 58, sección 39, bajo la rúbrica *"unlawful acts concerning computers"*, conductas como el fraude informático, divulgación de contraseñas, acceso lícito abusivo y acceso ilícito a ordenadores, y sistemas o redes informáticas[38]. Asimismo, también puede observarse el estatuto de Minnesota y más en concreto su capítulo 609, bajo la rúbrica *"criminal code"* o Código Criminal, las secciones 86, 87, 88, 89, 8912 y 8913, relativas a los delitos informáticos[39]. Por último, puede mencionarse el estatuto de Nevada, en concreto, su capítulo 205 que, bajo el título de *"unlawful acts regarding computers and information services"*, recoge la normativa relativa a los delitos informáticos en sus secciones 473 a 513[40].

2. Canadá

Canadá es un estado federal y, como nación, no es solo peculiar por la convivencia en un mismo territorio de dos lenguas, como son el inglés y el francés, sino que además, conviven y coexisten dos sistemas legales, conocidos como *civil law* o derecho

[37] ROVIRA DEL CANTO, E., *op.cit.*, pág. 345.
[38] Vid.http://kslegislature.org/li_2016/b2015_16/statute/021_000_0000_chapter/021_058_0000_article/01_058_0039_section/021_058_0039_k/ (consulta 15 de junio de 2017).
[39] Vid. https://www.revisor.mn.gov/statutes/?id=609 (consulta 15 de junio de 2017).
[40] Vid. http://www.leg.state.nv.us/NRS/NRS-205.html (consulta 15 de junio de 2017).

continental (de tradición romana implantado sobre todo en Quebec, la zona francófona de Canadá) y el *common law* de origen anglosajón[41], sistemas que, sin embargo, se encuentran subordinados a la norma suprema canadiense, la Constitución Canadiense o *Constitution of Canada*[42].

Se configura además el sistema legal canadiense como un sistema dual en cuanto a la jurisdicción, que podría denominarse como "bijurisdiccional", dividiéndose principalmente en, por un lado, derecho público o *public law*, el cual incluye los denominados como *criminal law* (derecho criminal relativo a los crímenes y las penas correspondientes por los mismos), *constitutional law* (que regula el gobierno, la relación del mismo con las distintas provincias y limita el poder gubernamental sobre los individuos a través de la protección de los derechos humanos y las libertades fundamentales, entre otros) y el *administrative law* o derecho administrativo, y por otro lado, el derecho privado o *private law*, que básicamente se limita a regular las relaciones entre los individuos. Siendo las competencias legislativas del *public law* mantenidas principalmente por el Estado, y las del *private law*, por las diferentes provincias de Canadá[43], competencias que se regulan por el *Constitution Act* de 1867, en su sección VI, que bajo la fórmula *Distribution of Legislative Powers*, regula la distribución de competencias entre el Parlamento y las provincias de Canadá, más concretamente, por la sección 91 (bajo el título *Powers of the Parliament*, las competencias del estado), por la sección 92 (bajo el título de *Exclusive Powers of Provincial Legislatures*, las competencias de las distintas provincias de Canadá), exponiendo los siguientes artículos de dicha sección algunas cuestiones de competencia, regulándose en las secciones 94A y 95 las competencia compartida (en materias como agricultura, inmigración o pensiones)[44].

Sin embargo, como se expuso, y en atención a lo dispuesto por la sección 91(27) del *Constitution Act* de 1867, recae el *public law* sobre el gobierno federal de Canadá, y a diferencia de los Estados Unidos de América, las provincias no gozan de competencias en materia criminal, siendo de aplicación al conjunto de ciudadanos las normas promulgadas por el Estado en esta materia. Canadá goza de una codificación en materia

[41] https://www.justice.gc.ca/eng/csj-sjc/just/03.html (consulta 1 de diciembre de 2018).
[42] https://www.justice.gc.ca/eng/csj-sjc/just/05.html (consulta 1 de diciembre de 2018).
[43] https://www.justice.gc.ca/eng/csj-sjc/just/02.html (consulta 1 de diciembre de 2018).
[44] https://laws-lois.justice.gc.ca/eng/const/ (consulta 1 de diciembre de 2018).

criminal denominada como *The Criminal Code*, que sin embargo, no engloba toda la legislación en esta materia, debiendo acudir en ocasiones a otras leyes.

Se hace relevante en materia de la regulación de los ciberdelitos la mención del *Criminal Law Amendment Act* [45]de 1985 y del *Protecting Canadians from Online Crime Act*[46] del año 2014 por los que se enmienda el *Criminal Code* en materia del cibercrimen.

Así, recoge el *Criminal Code*, dispersando a lo largo de su texto figuras relativas a la delincuencia informática:

La sección 162 recoge los supuestos de Voyeurismo, es decir, aquella conducta en la que se busca la obtención de una excitación sexual mediante la observación de personas desnudas o que realizan prácticas sexuales, penando el *Criminal Code* a quien, realizando dicha conducta de forma subrepticia, observe incluso mediante medios mecánicos o eléctricos (como, por ejemplo, una webcam conectada a un ordenador), o bien realice grabaciones de dichos actos cuando la otra persona esperaba de forma racional una cierta privacidad. Castigándose igualmente (por el apartado 4) la impresión, copia, publicación, distribución, circulación, venta, puesta a disposición, entre otras formas de difusión del material obtenido, cuando se sabe de su procedencia ilícita.

La sección 162.1 del *Criminal Code* tipifica la conducta relativa a la publicación, distribución, transmisión, puesta a disposición, así como conductas análogas, de imágenes de contenido íntimo o sexual sin consentimiento.

La sección 163 del *Criminal Code* recoge los supuestos relativos a los casos de *corrupting moral*s, es decir, lo que podría llamarse corrupción de la moral, recogiéndose en especial por su apartado (2) lo supuestos de realización de pornografía infantil, (3) la distribución y análogas de dicho material, (4) posesión de pornografía infantil, (4.1) acceso a tal contenido, donde las nuevas tecnologías juegan un papel importante respecto de dichas conductas.

Como mero apunte, la sección 168 tipifica los supuestos de *mailing obscene matter*, es decir, de uso de servicios de mensajería para enviar o transmitir material obsceno; sin embargo, si bien podría mal interpretarse la expresión *mails* debido a que en

[45] WILLIAMS SHARON, A., *"The Criminal Law Amendment Act 1985: Implications for International Criminal Law", Canadian Yearbook of International Law,* número 23, 1985, págs. 226 a 245.
[46] https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2014_31/page-1.html#docCont (consulta 1 de diciembre de 2018).

la versión francesa del texto se utiliza la expresión *la poste* (expresión para referirse a la oficina de correos), debido al uso de la expresión t*ransmitting*[47] o en el texto francés, *transmettre*, se desprende la posibilidad de punición de aquellas conductas que empleen servicios de mensajería electrónica para enviar dicho contenido.

Recoge la sección 171.1 del *Criminal Code*, supuestos de lo que podríamos denominar como facilitación de la disponibilidad de material sexual a menores; por otro lado, la sección 172.1 del Criminal Code penaliza los supuestos relativos al *luring child*, o corrupción de menores por medios informáticos o telemáticos, así como la sección 172.2 que recoge los delitos sexuales contra menores también mediante medios informáticos o de telecomunicación.

La sección 184 y siguientes del *Criminal Code* recoge los supuestos de interceptación ilícita de comunicaciones mediante dispositivos electromagnéticos, acústicos, mecánicos, de telecomunicaciones, o de cualquier otro tipo, debiendo ser destacadas la sección 191 del mismo texto, que tipifica los supuestos de posesión, venta o compra de los citados dispositivos o de sus componentes sabiendo que se diseñan especialmente para la interceptación ilícita de comunicaciones; y la sección 193 relativa al *disclosure of information* o a la divulgación de la información obtenida en los términos anteriormente expuestos.

La sección 326 del *Criminal Code* recoge los supuestos de *theft of telecommunication service*, es decir, de robo o defraudación de servicios de telecomunicaciones, y al hilo del anterior, la sección 327 encuadra los supuestos de posesión, creación, venta, ofrecimiento de venta de dispositivos o mecanismos diseñados para la realización de la conducta recogida por la sección 326 ya mencionada.

La sección 342 (3) del *Criminal Code* penaliza los supuestos de uso no autorizado de tarjetas de crédito, y en este sentido, cabe destacar la figura tipificada por la sección 342.01, en tanto recoge los supuestos de creación, reparación, compra, venta, exportación, importación, posesión de instrumentos, dispositivos, aparatos, materiales, y demás, cuando conozcan que han sido usados o sepa que se encuentran adaptados para su uso respecto de las conductas recogidas por la sección 342 (3) ya citada.

[47] https://dictionary.cambridge.org/dictionary/english/transmit (consulta 1 de diciembre de 2018).

La sección 342.1 del *Criminal Code* regula los supuestos de *unauthorized use of computer*, es decir, de uso ilícito de computadoras, así como la sección 342.2 regula los supuestos de realización, posesión, venta, ofrecimiento en venta, importación, obtención para su uso o distribución de medios o dispositivos designados para la realización de la conducta de la sección 342.1 ya citada, y la sección 430 del mismo texto.

Tipifica la sección 371 del *Criminal Code* los supuestos relativos a los *message in false name*, es decir, en los que el sujeto manda, con la intención de estafar, mensajes bajo la identidad de otra; y las secciones 372 (1), (2), y (3) recogen los supuestos de informaciones falsas, comunicaciones indecentes y de acoso mediante medios de telecomunicación.

La sección 381 del *Criminal Code* recoge los supuestos relativos al *using mails to defraud*, es decir, de defraudaciones mediante el uso de *mails.*

Las secciones 402.1 y siguientes regulan los supuestos de *identify theft*, es decir, supuestos de obtención o posesión de información identificativa (como por ejemplo, nombre de usuario y contraseña de una cuenta) en circunstancias que permiten inferir razonablemente que se pretende de su obtención o posesión la comisión de fraude, engaños o falsedades, debiendo destacarse igualmente la figura del apartado (2) de dicha sección, relativa al tráfico de dicha información identificativa.

La sección 430 del *Criminal Code* recoge la figura del *mischief*, es decir del daño, y en concreto, por su apartado (1.1), los supuestos de *mischief in relation to computer data*, es decir, de los daños en relación con los datos informáticos.

Por último, la sección 457 del *Criminal Code* penaliza los supuestos de falsificación de billetes bancarios, recogiendo la prohibición de creación, publicación, impresión, distribución o circulación de dichas falsificaciones, incluyendo por medios electrónicos, sistemas informáticos, y semejantes.

3. Alemania

Los delitos informáticos se encuentran tipificados en el *Strafgesetzbuch* o Código Penal de Alemania (en adelante stGB), bien mediante la consideración de los tipos tradicionales en atención a los nuevos medios de comisión empleados (internet y las plataformas informáticas), como ocurre con delitos como la incitación del odio del

parágrafo 130 stGB, y del parágrafo 184 en relación con el 184d *stGB* y los parágrafos 185 y 186 stGB en lo referente al insulto y la difamación[48]. Por otro lado, se tipifican de forma independiente tipos relativos a la delincuencia informática. Así, pueden apreciarse los parágrafos 149.1.1 stGB en lo relativo a los actos preparatorios para la comisión de falsificaciones mediante programas informáticos o similares; parágrafo 202.a stGB relativo al espionaje informático; 202.b stGB referente al *phishing*; 202.c stGB relativo a los actos preparatorios para la comisión de espionaje informático y *phishing*; 263 referente a la estafa informática; 269 stGB relativo a la falsificación de datos de prueba; 270 stGB en lo relativo al engaño en el procesamiento de datos; 271 stGB en lo referente a la introducción de entradas erróneas en registros públicos; 274.2 stGB relativo a la destrucción de documentos con intención de perjudicar a otro en relación con el parágrafo 202.a stGB; 303.a stGB relativo a la alteración de datos; y 303.b stGB relativo al sabotaje informático.

4. Italia

Sanciona el *Codice Penale* los delitos informáticos siguiendo un criterio muy similar al de Alemania y España, dispersando dichos tipos a lo largo del mismo. Pueden observarse así los siguientes preceptos del *Codice Penale* relativos a la delincuencia informática:

El artículo 270, prevé un incremento de la pena en caso de utilización de sistemas informáticos o telemáticos en casos de adiestramiento o actividades con fines de terrorismo.

Al igual que el artículo anterior, el artículo 320, relativo a la incitación a la comisión de delitos premeditados, también incrementa la pena al utilizar sistemas informáticos o telemáticos. En el mismo sentido, el artículo 421, relativo a la incitación a la delincuencia, aumenta la pena por la utilización de los citados sistemas.

El artículo 461, relativo a la fabricación o posesión de instrumentos para la falsificación de moneda, sellos o papel con filigrana, tipifica la fabricación, adquisición o posesión de programas informáticos para estos fines.

[48] PÉREZ MACHIO, A.I, *"Consideraciones de derecho comparado: la proyección de la normativa internacional en el tratamiento penal de la delincuencia informática"* en *Derecho penal informático*, Civitas, Navarra, 2010, pág. 152.

El artículo 615 ter tipifica las conductas relativas al acceso no autorizado a sistemas informáticos o telemáticos.

El artículo 615 quater recoge la posesión y distribución no autorizadas de códigos de acceso a sistemas informáticos o telemáticos.

El artículo 615 quinquies tipifica la distribución de equipos, dispositivos o programas informáticos destinados a dañar o detener sistemas informáticos o telemáticos.

El artículo 617 quater, relativo a la interceptación, impedimento o interrupción ilícita de comunicaciones informáticas o telemáticas.

El artículo 617 quinquies recoge en su redacción los supuestos de instalación de equipos diseñados para la intercepción, impedimento o interrupción de comunicaciones informáticas o telemáticas.

El artículo 617 sexies tipifica la falsificación, alteración o supresión del contenido de las comunicaciones informáticas o telemáticas.

El artículo 623 bis, relativo a otras comunicaciones y conversaciones, que viene a exponer la aplicabilidad de lo dispuesto para las comunicaciones telefónicas, telegráficas, informáticas o telemáticas a cualquier otra comunicación realizada a distancia de sonido, imagen o datos.

El artículo 635 bis, precepto que versa sobre los daños a información, datos y programas informáticos.

El artículo 635 ter, relativo al igual que el anterior a los daños a la información, datos o programas informáticos, pero en este caso, utilizados por el Estado, organismos públicos o en la prestación de servicios públicos.

El artículo 635 quater, relativo a los daños a sistemas informáticos o telemáticos.

El artículo 635 quinquies, que tipifica al igual que el anterior los daños a sistemas informáticos o telemáticos de carácter público.

El artículo 640 ter, que bajo la expresión *"Frode informática"* recoge la estafa informática y, a diferencia de nuestro Código penal, realiza una tipificación independiente del tipo básico de estafa, recogida por el artículo 640 bajo la rúbrica *"Truffa";* además, se evita la alusión a la fórmula "manipulación informática" como ocurre en nuestro

Código Penal, utilizando así la expresión "alteración de funcionamiento del sistema informático o telemático".

Por último, el artículo 640 quinquies recoge el fraude informático por el sujeto que presta servicios de certificación de firma electrónica.

5. Francia

Al igual que ocurría en países anteriormente analizados, se diseminan los delitos informáticos a lo largo del *Code Pénal* francés, si bien es cierto que en el mismo existen capítulos que referencian de forma expresa y engloban bajo una misma sección o capítulo un conjunto de delitos informáticos; en concreto, la sección 5ª del capítulo VI, título II, libro II del *Code Pénal*, relativo a *"des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques",* es decir, a los atentados a los derechos de la persona resultado de los ficheros o tratamientos informáticos, y en el mismo sentido, el capítulo III, título II, del libro III, relativo a *"des atteintes aux systèmes de traitement automatisé de données"*, es decir, a los ataques a sistemas automatizados de procesamiento de datos.

El artículo 222-28.6º del *Code Pénal* recoge un supuesto agravado respecto de las agresiones sexuales distintas a la violación por el uso de difusión de mensajes destinados a un público indeterminado mediante redes de telecomunicaciones.

El artículo 222-33-3 del *Code Pénal* tipifica supuestos de complicidad en la violación de la integridad de la persona (respecto de los artículos 222-1 a 222-14-1, 222-23 a 222-31 y 222-33) a los que registran por cualquier medio, y en cualquier soporte, imágenes relativas a la comisión de tales infracciones, penándose la difusión de las mismas. No siendo aplicable el artículo cuando dicha grabación o transmisión provenga del ejercicio normal de una profesión, con el fin de informar al público o con motivo de utilización como prueba en los tribunales.

El artículo 225-4-2.3º del *Code Pénal* prevé igualmente un subtipo agravado en los supuestos de trata de seres humanos para el caso de puesta en contacto gracias a la utilización de redes de telecomunicaciones y dirigiéndose a un número indeterminado de personas.

El artículo 225-7.10º del *Code Pénal* recoge un supuesto agravado para el caso del proxenetismo para el caso en que se empleen medios para la distribución de mensajes a un público indeterminado en redes de comunicación electrónica.

Se prevén por los artículos 226-1 a 226-3 del *Code Pénal* delitos contra la intimidad, en concreto, la captura, grabación o transmisión de voz o imágenes, así como los supuestos de uso de tal información, recogiendo igualmente los supuestos referidos de contenido sexual, transmitidos o expuestos al público sin consentimiento. En relación a lo expuesto artículos R226-1 a R226-12.

El *Code Pénal*[49] recoge en su sección 5ª, capítulo VI título II, libro II, y más concretamente en su artículo 226-4-1. 2º, los supuestos de robo de la identidad digital (en su párrafo segundo), y en el artículo 226-15 del mismo texto, los atentados contra el secreto de la correspondencia, en concreto, en su párrafo segundo, la intercepción de correspondencia emitida, transmitida o recibida por telecomunicaciones, o bien, instalando aparatos concebidos a tal fin; además, se recoge por los artículos 226-16 a 226-24 del *Code Pénal* los supuestos de *"des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques",* es decir, relativo a los atentados a los derechos de la persona resultado de los ficheros o tratamientos informáticos.

El artículo 227-22 del *Code Pénal* recoge un supuesto agravado para el caso de corrupción de menores cuando el menor haya entrado en contacto con el autor gracias a la utilización por el mismo de una red de comunicaciones electrónicas para la difusión de mensajes destinados a un público indeterminado.

El artículo 227-23 del *Code Pénal* recoge igualmente un supuesto agravado respecto de la toma de imágenes, grabación o transmisión de imágenes o representaciones de menores para los casos en los que se empleen medios de comunicación electrónica para su difusión.

El artículo 227-26.4º del *Code Pénal* recoge un supuesto agravado respecto de los atentados sexuales contra menores cuando el menor se pone en contacto con el autor gracias a la utilización por el mismo de medios de comunicación electrónica dirigiéndose a un público indeterminado.

[49]https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (consulta 7 de diciembre de 2018).

Por otro lado, el artículo 322-6-1 del *Code Pénal* recoge respecto de la difusión por cualquier medio, salvo a profesionales, de procedimientos que permitan la fabricación de artefactos de destrucción, un supuesto agravado para el caso en el que se empleen medios de comunicación electrónica para su difusión a un público indeterminado. Ha de recalcarse en este sentido, que el legislador francés, para la construcción de los supuestos agravados, suele utilizar la fórmula *"réseau de communication électronique à destination d'un public non déterminé"*, lo cual podría traducirse como "red de comunicación electrónica para un público no especificado".

Se promulgó en el año 1988 la conocida como *loi Godfrain*[50] o *loi nº 88 du janvier 1988 relative à la fraude informatique*[51], en materia de fraude informático, que introdujo dentro del título II del libro III un capítulo III que rezaba *"de certaines infractions en matière informatique"* (artículos 462-2 a 462-9), recogiendo así diversos supuestos relacionados con la informática, como el acceso fraudulento a sistemas, daños informáticos, falsificación de documentos informatizados entre otros; sin embargo, en la actualidad, y de conformidad con la misma, se recogen por el *Code Pénal*, más concretamente, en su libro III, título II, capítulo III, los delitos relativos a *"es atteintes aux systèmes de traitement automatisé de données"*, es decir, a los ataques a sistemas automatizados de procesamiento de datos, figuras como el acceso o permanencia fraudulenta en un sistema automatizado de procesamiento de datos, la supresión o modificación de datos contenidos en el sistema (artículo 323-1), la obstaculización o distorsión del funcionamiento de un sistema automatizado de procesamiento de datos (artículo 323-2), la introducción, modificación o supresión fraudulenta de datos en un sistema automatizado de procesamiento de datos (artículo 323-3), la importación, tenencia, ofrecimiento, cesión o puesta en disposición de equipamiento, un instrumento, un programa informático o cualquier dato concebidos o especialmente adaptados para cometer una o varias de las infracciones previstas (artículo 323-3-1, incluido al *Code Pénal* en atención a *la loi pour la confiance dans l'économie numérique, no 2004-575 du 21 juin 2004*), la participación en un grupo formado o en un acuerdo establecido para la preparación, plasmada en uno o varios hechos materiales de las infracciones previstas (artículo 323-4), supuestos de actuación en grupo organizado en contra de sistemas de procesamiento automatizado de datos (artículo 323-4-1), supuestos de comisión por

[50] ROVIRA DEL CANTO, E., *op.cit.*, pág. 388.
[51] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419 (consulta 7 de diciembre de 2018).

persona física de los delitos expuestos (artículo 325-5), supuestos de personas jurídicas culpables (artículo 323-6), y supuestos imprudentes (artículo 323-7).

El artículo 411-9 del *Code Pénal* recoge la figura del sabotaje de sistemas de procesamiento automatizado de datos atentando contra intereses de la Nación.

El artículo 421-1 2º del *Code Pénal* dispone que constituyen actos de terrorismo las infracciones en materia de informática cometidos intencionalmente en relación a una acción individual o colectiva que tenga por objeto alterar gravemente el orden público.

El artículo 421-2-5 del *Code Pénal* recoge un supuesto agravado para los actos de extracción, reproducción o trasmisión intencional de datos que provoquen al terrorismo o hagan apología del mismo de forma pública, cuando los hechos se cometieren mediante el uso de servicios de comunicación en línea.

Los artículos 411-6 a 411-8 del *Code Pénal* regulan la entrega de documentos o datos informatizados o ficheros susceptibles de atentar contra los intereses fundamentales de la nación a una potencia extranjera, a una empresa u organización extranjera o bajo su control o a el de sus agentes, y los artículos 413-9 a 413-12 del *Code Pénal* recogen los atentados contra secretos de la defensa nacional.

El artículo 432-9 del *Code Pénal* recoge los supuestos en los que se ordena, comete o facilita la interceptación o desvió de correspondencia emitida, transmitida o recibida por vía de medios de telecomunicación por una autoridad pública o encargada de una misión de servicio público, así como la realizada por agentes/operadores de redes de comunicación electrónica o de servicios de telecomunicación en el ejercicio de sus funciones, ordene, cometa o facilite la interceptación o desvío de la correspondencia transmitida.

Finalmente, se hace relevante mencionar la *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*[52], y más concretamente, su artículo 1, que reconoce la libertad de comunicación pública por medios electrónicos, limitándose únicamente el ejercicio de la misma en el respecto de la dignidad humana, la propiedad de otros, el orden público, entre otros, y su artículo 6, que recoge ciertos supuestos de responsabilidad penal de los administradores o prestadores de servicios de comunicación

[52]https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164 (consulta 7 de diciembre de 2018).

pública en línea (subapartados 3 y siguientes). En este sentido, igualmente referenciar los artículos R625-10 a R625-13, relativos a *"des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques"*.

6. Irlanda

La República de Irlanda emplea un sistema de *common law*, y por ende, no puede olvidarse, pese a lo que se expondrá a continuación, la gran relevancia en este tipo de sistemas de las resoluciones judiciales, al ser el sistema de fuentes del derecho distinto del modelo continental o de *civil law*. Irlanda, a diferencia de otros países, no ha publicado aun una codificación de su legislación en materia penal (pese a que se encuentra la misma en proceso), la cual se encuentra regulada principalmente por la *primary legislation*, es decir, los denominados *Acts of the Parliament o Acts of the Oireachtas* emanados del poder legislativo, el Parlamento Irlandés (también como *Oireachtas*), el cual es bicameral, y se encuentra compuesto por el *Dáil Éireann* o *House of Representatives* (Asamblea) y por el *Seanad Éireann* (Senado). Al hilo de lo anterior, y como ya se adelantaba, la legislación en Irlanda se divide principalmente en *primary legislation* y en *secundary legislation* (también denominada *statutory instruments*). Así, la *primary legislation* se encuentra formada por los Acts *of the Parliament* o *Acts of the Oireachtas*, los cuales emanan directamente del *Oireachtas, y* la *secundary legislation* o *statutory instruments (*puede tomar diversas formas, en concreto, *orders, regulations, rules, by-laws and schemes),* consiste en una legislación subrogada, es decir, en la que se confiere o delega por la *primary legislation* cierto poder legislativo a determinados sujetos, órganos o instituciones (por ejemplo, esta *staturory legislation*, es utilizada para implementar Directivas Europeas, entre otras)[53].

Como ya se mencionaba, Irlanda no ha realizado aun codificación de su legislación en materia penal, la cual se encuentra regulada principalmente por la *primary legislation*, más concretamente por los *Criminal Justice Act.* Ahora bien, en la parte 14, sección 167 y siguientes del *Criminal Justice Act 2006*[54], se hace referencia a la creación de un comité encargado de la codificación de legislación en materia criminal y la

[53] http://eur-lex.europa.eu/n-lex/info/info-ie/index_en (Consulta 11 de diciembre de 2018).
[54] http://www.irishstatutebook.ie/eli/2006/act/26/enacted/en/html?q=criminal+justice+act (consulta 11 de diciembre de 2018).

consecuente creación de un *criminal code*; sin embargo, el mismo no ha sido aún publicado, debiendo acudir en la actualidad a la muy diversa y dispersa normativa.

Así, se recogían por el denominado como *Criminal Damage Act* 1991[55] en su sección 5, relativa al *unauthorised accessing of data* o acceso no autorizado a datos, y por otro lado, el *Criminal Justice (Theft and Fraud Offences) Act, 2001*[56], que recoge en su sección 9ª la conducta relativa al *unlawful use of computer* o uso ilícito de computadores. Sin embargo, se publica en el año 2017 el *Criminal Justice (Offences Relating to Information Systems) Acts 2017*[57], que enmienda el ya citado *Criminal Damage Act 1991*, recogiéndose por el mismo las conductas relativas al acceso a sistemas de la información sin autorización (sección 2), interferencia de sistemas informáticos sin autorización (sección 3), interferencia de datos sin autorización (sección 4), interceptación de datos sin autorización (sección 4), interceptación en la transmisión de datos (sección 5), utilización de programas informáticos, contraseñas, códigos o datos con los propósitos expuestos en las secciones 2,3,4 o 5 (artículo 6), comisión por personas jurídicas o *body corporate* (artículo 9).

7. Reino Unido

Reino Unido, como Irlanda, mantiene un sistema de *common law*, y al igual que el citado Estado, no dispone de una codificación en materia criminal o penal, como si ocurre por ejemplo en Canadá, debiendo por ende, acudir a la diversa y diseminada legislación sobre la materia para su análisis; para ello, resulta muy útil el estudio realizado por el *Crown Prosecution Service*, conocido comúnmente como CPS, que bajo el título *"Cibercrime-prosecution guidance"*[58], de forma detallada, analiza la delincuencia informática en el Reino Unido y su regulación, análisis que, por otro lado, servirá de base para la exposición de la presente cuestión, y del cual se recomienda su lectura, puesto que debido a cuestiones espaciales, se abordara de una forma sintética la amplísima y dispersa legislación del Reino Unido en materia de delincuencia informática.

[55] http://www.irishstatutebook.ie/eli/1991/act/31/section/5/enacted/en/html#sec5 (consulta 11 de diciembre de 2018).
[56] http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/html?q=criminal+justice+act (consulta 11 de diciembre de 2018).
[57] http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html?q=criminal+justice+act+ (consulta 11 de diciembre de 2018).
[58]Cfr. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (consulta 10 de diciembre de 2018).

Se dividen los delitos informáticos o ciberdelitos por el *Crown Prosecution Service* en 2 categorías, por un lado los *Cyber-Dependent Crimes*, y por otro lado, los *Cyber-Enabled Crimes.* Definiéndose por el citado órgano los *Cyber-Dependent Crimes* como aquellos que únicamente pueden realizarse mediante el uso de las TIC (Tecnologías de la Información y las Comunicaciones), donde los dispositivos empleados pueden ser, tanto el medio o herramienta comisiva, como el objeto del delito, y, por otro lado, los denominados como *Cyber-Enabled Crimes*, que son aquellos delitos tradicionales que pueden incrementar su alcance o escala mediante la utilización de ordenadores, redes informáticas o de las TIC[59].

Así, el *Crown Prosecution Service* engloba en la categoría de *Cyber-Dependent Crimes* conductas como el hacking o uso de las tecnologías para robar datos personales, la manufactura o distribución de malware, manufactura y uso de Spyware, entre otras. Por otra parte, dentro de la categoría de los *Cyber-Enabled Crimes* se recogen, entre otras conductas, el cibercrimen económico (como los fraudes en comercio electrónico, ventas fraudulentas a través de subastas online, estafas informáticas, fraudes en el mercado, romances online o técnicas de persuasión con la intención de defraudar o engañar, delitos propiedad intelectual, falsificaciones informáticas), venta y compra de productos ilegales en línea, comunicaciones maliciosas (como las comunicaciones ofensivas, *ciberbulling*, *trolling*, *virtual mobbing)*, ofensas que afectan a objetivos específicos, incluyendo los ciberdelitos dirigidos contra las mujeres o los niños (como la divulgación de imágenes sexuales privadas sin consentimiento, *ciber-stalking*, *child grooming*, pornografía infantil, y caso de pornografía extrema u obscena).

Una vez analizado lo anterior, en relación a los *Cyber-Dependent Crimes* puede destacarse cierta normativa; así, por ejemplo, el *Computer Misuse Act 1990*[60] (de gran importancia en materia de cibercrimen), una ley concebida para establecer la seguridad del material informático contra accesos o modificaciones no autorizados y fines relacionados, siendo la sección 1 de dicho texto relativa a los accesos no autorizados a material informático; la sección 2 relativa al acceso no autorizado con la intención de cometer o facilitar la comisión de más delitos; la sección 3 relativa a los accesos no

[59] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (consulta 10 de diciembre de 2018).
[60] http://www.legislation.gov.uk/ukpga/1990/18#commentary-c19759931 (consulta 10 de diciembre de 2018).

autorizados intencionales o imprudentes que provoquen un perjuicio o deterioro en el funcionamiento de la computadora; la sección 3ZA relativa a los accesos no autorizados que causen o creen un riesgo de un daño grave; y la sección 3A relativa a creación, suministro u obtención de artículos para su uso en la realización de las conductas recogidas por las secciones 1, 3 o 3ZA. Igualmente, es destacable el *Regulation of Investigatory Powers Act 2000*[61], que tipifica los supuestos de intercepción ilícita de las comunicaciones, y la adquisición y divulgación de datos relacionados con las comunicaciones, entre otras conductas, recogiéndose en su sección 1 el concepto de intercepción ilícita, y en su sección 2, el significado del concepto intercepción. También son mencionables, por un lado, la sección 327 del *Proceeds of Crime Act 2002*[62], situada en la parte 7 de dicho texto, relativa a los delitos de blanqueo de capitales, y por otro lado, las secciones 55, 170 y siguientes del *Data Protection Act 2018*[63], por el que se castigan la obtención ilícita de datos personales, y la identificación de datos personales no identificados sin el consentimiento del controlador o responsable de la desidentificación de los mismos.

Son igualmente destacables las secciones 1, 2, y sobre todo 6, 7 y 8 del *Fraud Act 2006*[64], relativas a la posesión, la creación, adaptación, oferta, la distribución o abastecimiento y demás conductas análogas, de artículos para su uso en defraudaciones.

No obstante, se hace igualmente mencionable la sección 1 del *Criminal Law Act 1977*[65] en materia de conspiración, y las secciones 44 a 46 del *Serious Crime Act 2007*[66] en relación con la sección 11A Y 12 (*computer misuse* y *intellectual property*), de la parte primera del Shedule 1, relativo a las *"serious offences in England and Wales"*, que versan sobre las formas intencionales de alentar o ayudar en la comisión de un delito.

Asimismo, si bien cierto de lo ya expresado respecto de los *Cyber-Dependent Crimes* se hace igualmente aplicable para los *Cyber-Enabled Offences*, se habrá de profundizar en aquella legislación más específica en la materia; así, por ejemplo, en materia de propiedad intelectual, las secciones 107 (relativa a la responsabilidad penal

[61] https://www.legislation.gov.uk/ukpga/2000/23 (consulta 10 de diciembre de 2018).
[62] https://www.legislation.gov.uk/ukpga/2002/29 (consulta 10 de diciembre de 2018).
[63] http://www.legislation.gov.uk/ukpga/2018/12/enacted (consulta 10 de diciembre de 2018).
[64] https://www.legislation.gov.uk/ukpga/2006/35 (consulta 10 de diciembre de 2018).
[65] https://www.legislation.gov.uk/ukpga/1977/45 (consulta 10 de diciembre de 2018).
[66] https://www.legislation.gov.uk/ukpga/2007/27 (consulta 10 de diciembre de 2018).

por hacer o comerciar con ilícitos), 198 (relativa a la responsabilidad penal por realizar, tratar o utilizar grabaciones ilícitas), 296 a 299 (relativa a los aparatos diseñados para eludir las medidas de protección, fraudes en la recepción de las transmisiones, protección de las bases de datos y programas informáticos, entre otros) del *Copyright, Designs and Patents Act* 1988[67]; igualmente, la sección 92 del *Trade Marks Act 1994*[68], relativa a los casos de uso no autorizado de marcas comerciales, debiendo recalcar su apartado (3) en cuanto recoge los supuestos de fabricación, posesión, de dispositivos específicamente diseñados o adaptados para hacer copias de un signo idéntico a una marca registrada, e incluso, el saber o tener motivos para creer que se ha utilizado, o se va a utilizar, para producir las citadas copias, y las secciones 9 a 14 of the *Video Recordings Act 1984*[69], relativas a la posesión, suministro de videos o grabaciones de trabajos sin certificado de clasificación, con falsas indicaciones de clasificación, o sin la correspondiente licencia, entre otras.

Al hilo de lo anterior, y respecto de la falsificación, las secciones 1 a 10 del *Forgery and Counterfeiting Act 1981*[70] (sobre todo la sección 8 (1)(d) en cuanto refiere como instrumento, de falsificación, cualquier disco, cinta, pista de sonido u otro dispositivo en el que la información se graba o almacena por medios mecánico, electrónicos u otros), y las secciones 4 a 6 del *Identity Document Act 2010*[71], relativas a los aparatos designados o adaptados para la realización de documentos de identidad falsos.

Respecto de las comunicaciones ofensivas, la sección 1 del *Malicious Communications Act 1988*[72], relativa a la punición de comunicaciones (incluyendo las electrónicas) con ánimo de causar ansiedad o estrés, como amenazas, mensajes groseros u ofensivos, así como informaciones falsas, y las secciones 125 y siguientes del *Communications Act 2003*[73], relativas a los delitos relacionados con redes y servicios, tipificando conductas como la obtención deshonesta de servicios de comunicaciones electrónicas, la posesión o suministro de aparatos al fin anteriormente expuesto y el uso inapropiado de redes electrónicas de comunicación pública. Mencionables igualmente las

[67] https://www.legislation.gov.uk/ukpga/1988/48 (consulta 10 de diciembre de 2018).
[68] https://www.legislation.gov.uk/ukpga/1994/26 (consulta 10 de diciembre de 2018).
[69] https://www.legislation.gov.uk/ukpga/1984/39 (consulta 10 de diciembre de 2018).
[70] https://www.legislation.gov.uk/ukpga/1981/45 (consulta 10 de diciembre de 2018).
[71] http://www.legislation.gov.uk/ukpga/2010/40/enacted (consulta 10 de diciembre de 2018).
[72] https://www.legislation.gov.uk/ukpga/1988/27 (consulta 10 de diciembre de 2018).
[73] https://www.legislation.gov.uk/ukpga/2003/21 (consulta 10 de diciembre de 2018).

secciones 1 a 5 del *Protection from Harassment Act 1997*[74], donde se recogen disposiciones relativas a la punición del acoso, como, por ejemplo, los supuestos de *stalking*.

En materia de violencia y delitos sexuales contra la mujer, destacar las secciones 32 a 35 y el *Schedule* 8 del *Criminal Justice and Courts Act 2015*[75], *Shedule* 8 en concreto, en lo relativo a los supuestos de divulgación de fotografías o películas sexuales privadas, así como en materia de abuso doméstico, las secciones 76 y 77 del *Serious Crime Act 2015*[76], relativas a abuso doméstico, y en concreto, a los comportamientos de control o coercitivos en el seno de una relación íntima o familiar. Igualmente, la sección 67 del *Sexual Offences Act 2003*[77], relativa a los supuestos de voyeurismo, y más concretamente, su apartado (4), que recoge los supuestos de instalación, construcción o adaptación de equipos o partes de los mismos con la intención de facilitar la comisión de estas conductas a sí mismo o a otras personas.

Respecto de los delitos sexuales contra menores, destacar las secciones 1 a 7 del *Protection of Children Act 1978*[78], relativas a las conductas de realización o permisión de la misma, distribución, reproducción, posesión o publicación de fotografías o pseudofotografías indecentes de menores, todo ello en relación a las secciones 160 y 161 del *Criminal Justice Act 1988*[79], las secciones 45 y 46 del *Sexual Offences Act 2003*, y las secciones 69 y 70 del *Criminal Justice and Immigration Act 2008*. Igualmente relevantes, al hilo de lo anterior, son las secciones 12, 14 y 15 del *Sexual Offences Act 2003* en relación con la Sección 36 del Criminal Justice and Courts Act 2015, relativas a los delitos sexuales contra menores que, en concreto, recogen las conductas de exposición a un menor a la observación de actos sexuales, delitos sexuales contra menores cometidos por menores o adolescentes, la facilitación de la comisión de los citados actos, así como los supuestos conocidos como *child grooming*, es decir, supuestos de comunicación con menores con fines sexuales. También relevantes en este sentido, son las secciones 62 a 69 del *Coroners and Justice Act 2009*[80], relativo a la posesión de imágenes prohibidas no necesariamente fotográficas de menores.

[74] https://www.legislation.gov.uk/ukpga/1997/40 (consulta 10 de diciembre de 2018).
[75] http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted (consulta 10 de diciembre de 2018).
[76] http://www.legislation.gov.uk/ukpga/2015/9/contents/enacted (consulta 10 de diciembre de 2018).
[77] https://www.legislation.gov.uk/ukpga/2003/42 (consulta 10 de diciembre de 2018).
[78] https://www.legislation.gov.uk/ukpga/1978/37 (consulta 10 de diciembre de 2018).
[79] https://www.legislation.gov.uk/ukpga/1988/33/contents (consulta 10 de diciembre de 2018).
[80] https://www.legislation.gov.uk/ukpga/2009/25/contents (consulta 10 de diciembre de 2018).

Y, respecto de la pornografía extrema y de las publicaciones obscenas, las secciones 63, 67 y 71 del *Criminal Justice and Immigration Act 2008*[81], en relación con la sección 38 del *Criminal Justice and Courts Act 2015*, e igualmente, en relación a los supuestos de pornografía obscena, se hace destacable el *Obscene Publications Act 1959*[82].

IV. Marco de estudio específico: los delitos informáticos que inciden sobre el bien jurídico patrimonio

Sección 1ª: La estafa informática

1. Concepto y denominación

Se habla a continuación, como ya se mencionó en apartados anteriores, del delito informático por excelencia, el cual, dada su incidencia, goza de una cierta relevancia dentro de la esfera pública y ha sido objeto en numerosas ocasiones de declaraciones realizadas por los medios de comunicación[83], lo cual no deja de manifestar quizá una relativa preocupación social acerca de este tipo de conductas. En la actualidad, la comisión de este tipo de delitos ha sufrido un aumento considerable, y ello es debido quizá a factores como la escasa inversión requerida para la realización de estas conductas, el aparente anonimato que ofrece internet o la evasión de una confrontación directa con la víctima como sucedía en la estafa tradicional, entre otras posibles causas.

Queda recogido el tipo de estafa informática en el artículo 248.2.a) del Código Penal y expone en concreto que serán considerados como reos de estafa *"los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".* Consiste, por tanto, la estafa informática en lograr, a través del uso de la informática, la transferencia no consentida de un activo patrimonial mediante la manipulación o conductas similares a la misma de sistemas informáticos y de telecomunicaciones sin la necesidad de engañar a ninguna persona, como sí ocurre en la

[81] https://www.legislation.gov.uk/ukpga/2008/4/contents (consulta 10 de diciembre de 2018).
[82] https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents (consulta 10 de diciembre de 2018).
[83] http://www.antena3.com/noticias/economia/cada-vez-mas-espanoles-compran-traves-internetaumentan-estafas-online_20151228571b5e804beb287a291798c5.html , (consulta 15 de junio de 2017).

estafa tradicional[84]. En el sentido de lo anterior, expone el Tribunal Supremo en su STS 860/2008, de 17 de diciembre, que, *"cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2 del Código penal. También cuando se emplea un artificio semejante".*

Y si bien en la actualidad parece más o menos clara la naturaleza de estas conductas, ello se cuestionó antaño al entender un sector doctrinal que la naturaleza de las mismas se acercaba más al hurto que a las defraudaciones; en este sentido, parece necesario citar a CONDE-PUMPIDO FERREIRO en cuanto expone que *"algunos afirman que en tales casos lo que se da es hurto, pues se está «tomando» algo sin la voluntad de su dueño, ya que […], la máquina carece también de voluntad y lo que «entrega», ante la manipulación del agente, lo hace automáticamente, esto es, sin consentimiento o sin «voluntad de su dueño». Pero ello no sirve para asumir todos los tipos de fraude informático, pues a veces estos no se dirigen a obtener la entrega de una cosa […] sino a evitarla, esto es, a disminuir el importe económico de un crédito o del total de la mercancía a entregar o el importe de una suma a pagar, con lo que no se produce una sustracción sino un fraude"*[85], exponiendo además que, mientras el dinero no se materialice en un soporte físico, es decir, en tanto se represente como una mera anotación en la entidad bancaria, difícilmente podrá tener carácter de cosa mueble y que, por ende, no sería entendible la subsunción de la conducta como hurto[86]. Lo que es manifiesto en todo caso es que, de la voluntad del legislador, se desprende la naturaleza de defraudación de estas conductas ello en atención a la ubicación del precepto dentro del Código Penal.

Al igual que ocurría con la terminología "delito informático", no existe un consenso o unanimidad en la doctrina respecto a la denominación del presente tipo, refiriéndose a éste como *"manipulaciones informáticas defraudatorias patrimoniales"*[87],"*fraude informático"*[88], *"fraude por medios informáticos"*[89], *"estafa*

[84] SUAREZ-MIRA RODRIGUEZ, C., JUDEL PRIETO, A., PIÑOL RODRIGUEZ, J.R., *Manual de derecho penal, tomo II (parte especial)*, Civitas, Navarra, 2011, pág. 265.
[85] CONDE-PUMPIDO FERREIRO, C., *Estafas*, Tirant lo Blanch, Valencia, 1997, pág. 214.
[86] *Ídem.*
[87] ROVIRA DEL CANTO, E., *op.cit.*, pág. 558.
[88] QUERALT JIMÉNEZ, J.J., *Derecho Penal Español Parte Especial*, Tirant lo Blanch, Valencia, 2015, pág. 552.
[89] POLAINO NAVARRETE, M., *et alii*, *Lecciones de Derecho Penal Parte Especial Tomo II*, Tecnos, Madrid, 2011, pág. 98.

informática"[90], *"estafa por medios informáticos"*[91], *"estafa mediante manipulaciones informáticas"*[92] , *"estafas por computación"*[93] y *"estafas por computador"*[94], entre otras. Pese a la amplia terminología expuesta con anterioridad, se opta en el presente trabajo por la denominación "estafa informática" en atención a la ubicación del precepto en el capítulo VI, *"de las defraudaciones"*, y, de forma más concreta, dentro de la sección 1ª del mismo, bajo la rúbrica "De las estafas"[95]. Dicha tesis puede verse apoyada por el empleo de dicha terminología por autores como MATA Y MARTÍN y REY HUIDOBRO[96] entre otros, y por el propio Tribunal Supremo en sentencias como la STS 369/2007, de 9 de mayo, cuando expresa que *"llegados a este punto habrá de determinarse si estas operaciones pueden ser comprendidas en la actual estafa informática del art. 248.2"*; en el mismo sentido la STS 948/2002, de 8 de julio, cuando expone que *"tal falsedad se consumiría en el delito de estafa informática (art. 248.2 CP");* de igual forma la STS 987/2012, de 3 de diciembre, cuando falla *"que debemos declarar y declaramos HABER LUGAR a los recursos de casación […] contra la sentencia dictada por la Sección Primera de la Audiencia Provincial de Guipúzcoa con fecha 28 de octubre de 2011 , que les condenó por un delito de estafa informática".*

2. Evolución normativa y regulación actual

El Proyecto de Ley Orgánica de 1980 recogía en su artículo 255 que *"cometen estafa los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero. La estafa se penará como delito cuando la cuantía de lo defraudado exceda de 15.000 pesetas o, aún sin exceder de esa cantidad, el culpable hubiere sido anteriormente condenado por delito contra el patrimonio de carácter lucrativo, o por dos o más faltas de igual clase"*. No se hacía ninguna referencia como puede apreciarse a la estafa

[90] MATA Y MARTÍN, R.M., *Delincuencia informática…*, págs. 37 y ss.
[91] GONZÁLEZ CUSSAC, J.L., *et alii*, *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2016, pág. 397.
[92] SERRANO GÓMEZ, A., SERRANO MAÍLLO, A., *Derecho Penal Parte Especial*, Dykinson, Madrid, 2009, pág. 435.
[93] CHOCLÁN MONTALVO, J.A, "*Fraude informático y estafa por computación"* en *Internet y derecho penal*, Consejo General del Poder Judicial, Madrid, 2001, págs. 321 y ss.
[94] LUZÓN CUESTA, J.M., *Compendio de Derecho Penal Parte Especial*, Dykinson, Madrid, 2015, pág. 190.
[95] ROVIRA DEL CANTO, E., *op.cit.*, pág. 558.
[96] REY HUIDOBRO, L.F, *"La estafa informática: relevancia penal del phising y el pharming", La Ley Penal*, número 101, 2013, pág. 5.

informática y no fue hasta el Proyecto de Ley Orgánica de 1992 cuando aparece ésta tipificada en su artículo 252, siendo su redacción la siguiente: *"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio propio o ajeno. 2. También cometen estafa los que, con ánimo de lucro, realizaren una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos, y así ocasionaren un perjuicio a otro"*. Es apreciable primero una división en apartados y no en párrafos como ocurría en el Proyecto de LO de 1980; segundo, la nueva redacción del tipo básico de estafa recogida en el apartado primero que ha sido mantenida hasta el día de hoy; y tercero, que se introduce en el apartado segundo el tipo de estafa informática con una redacción un tanto primaria, que sería modificada en el artículo 241 del Proyecto de Ley Orgánica de 1994 en cuanto disponía: *"2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero"*, redacción finalmente plasmada en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Se reformula el tipo respecto a la redacción ofrecida por el Proyecto de Ley Orgánica de 1992, por un lado manteniendo el concepto de manipulación informática, pero sin delimitarlo como sí ocurría en la redacción del año 1992, generando una excesiva amplitud conceptual criticada por determinados sectores doctrinales al entender su poca concreción, que al agregar además el concepto *"o artificio semejante"* otorga una mayor amplitud conceptual que no permite *a priori* la delimitación de las conductas abarcables por el tipo, pareciendo el legislador cubrir cualquier tipo de laguna de ley en un futuro.

En el marco comunitario es reseñable la Decisión Marco 2001/413/JAI, de 28 de mayo de 2001, relativa a la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, cuando en su artículo 3 refiere que *"cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros mediante: la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o la interferencia indebida en el funcionamiento de un programa o sistema*

informático", a la que parecía adecuarse ya la legislación española; y el artículo 2, en cuanto expone: *"cada Estado miembro deberá adoptar las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada, al menos con respecto a tarjetas de crédito, tarjetas eurocheque, otras tarjetas emitidas por entidades financieras, cheques de viaje, eurocheques, otros cheques y letras de cambio: b) falsificación o manipulación de instrumentos de pago, para su utilización fraudulenta",* que como se verá a continuación parece influir en la reforma operada por la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal.

Se produce, con la aprobación Ley Orgánica 15/2003, de 25 de noviembre, una modificación del Código Penal y, más concretamente por el artículo 82 de la misma, una modificación en el artículo 248 del Código Penal, agregando un tercer apartado con la siguiente redacción: *"3. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo."*, decisión del legislador que parece buscar una erradicación de este tipo de conductas de raíz, produciéndose así un adelantamiento de las barreras de protección. Con posterioridad, la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal, y más en concreto, su artículo 61, modifica de nuevo el artículo 248, volviendo a restructurarlo en 2 apartados con la salvedad de que el segundo de ellos se dividirá en 3 subapartados, siendo la nueva redacción y la vigente en la actualidad, la siguiente: *"2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"*, en este caso, parece el legislador poner fin a la discusión doctrinal relativa a la calificación de la utilización de tarjetas de crédito o débito, cheques de viaje o los datos obrantes en estos; sin embargo, baste esta mención de la cuestión para su análisis en posteriores apartados.

3. Bien jurídico protegido

Siguiendo una concepción Lisztiana del bien jurídico, arraigada en la doctrina mayoritaria, puede entenderse aquél como *"un concreto interés, valor o realidad valiosa, de una persona o de la sociedad, importante para la existencia y desenvolvimiento de éstas y que por ello merece protección jurídica"*[97]. Puede deducirse así de la anterior afirmación la existencia de bienes jurídicos individuales y colectivos; consisten los primeros en *"presupuestos que la persona necesita para su autorrealización y el desarrollo de su personalidad en la vida social"*[98], siendo así bienes jurídicos individuales la vida y la integridad, entre otros. Y se configuran como bienes jurídicos colectivos aquellos que *"afectan más a la sociedad como tal, al sistema social que constituye la agrupación de varias personas individuales y supone un cierto orden social o estatal"*[99], constituyendo así bienes jurídicos colectivos el medio ambiente, la salud pública, seguridad colectiva y el orden público, entre otros.

Desempeña el bien jurídico diversas funciones, como puedan ser la de limitación y orientación del *ius puniendi* o la de interpretación de la orientación y finalidad protectora de los tipos; sin embargo, en el presente trabajo, es necesaria la enfatización de la función sistemática del bien jurídico, siendo éste uno de los argumentos fundamentales para la determinación del bien jurídico protegido por el tipo de estafa informática[100]. Tal función sistemática es apreciable en el propio Código Penal, dado que se produce en éste una clasificación u ordenación de los distintos tipos en función del bien jurídico protegido por los mismos.

Parece en principio obvia la delimitación del bien jurídico protegido en la estafa informática, dada, primero, la situación del artículo 248.2 del Código Penal dentro del mismo y, en segundo lugar, el tenor literal del citado precepto. En este mismo sentido se expresaba ya ANTON ONECA respecto a las estafas: *"el ataque del estafador al patrimonio, bien jurídico protegido aquí, como en los demás preceptos sobre*

[97] LUZÓN PEÑA, D.M., *Lecciones de Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 2012, pág. 176.
[98] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 2010, pág. 60 y ss.
[99] *Ídem.*
[100] Cfr. LUZÓN PEÑA, D.M., *op.cit.*, pág. 178.

infracciones patrimoniales, es evidente, y si algunos autores no lo mencionan […] es porque dan aquel por supuesto, omitiendo lo genérico para subrayar lo específico"[101].

Se sitúa así el precepto en la sección 1ª del capítulo VI, título XIII, libro II del Código Penal, encuadrándose dentro de los delitos contra el patrimonio y contra el orden socioeconómico; parece así el legislador, mediante lo anteriormente mencionado, dejar clara la finalidad de protección del bien jurídico patrimonio mediante tal precepto. Puede mencionarse en este sentido la STS 860/2008, de 17 de diciembre, que, pese a referirse al tipo básico de estafa, es perfectamente extrapolable al tipo de estafa informática; expone así dicha resolución que "*es indudable, por su ubicación sistemática, que el bien jurídico que se protege en la estafa es el patrimonio"*.

Por otro lado, refiere el propio artículo 248.2 la necesidad de consecución de una *"transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"*, funcionando así el perjuicio patrimonial como un eje determinante de la consumación o no del tipo. A favor de la tesis expuesta se pronuncia REY HUIDOBRO: *"sin embargo, sin ser una estafa propiamente dicha, presenta importantes similitudes con la estafa (de ahí que se inserte en el art. 248 CP). Así, el bien jurídico protegido es el patrimonio (la referencia a cualquier activo patrimonial como objeto material sobre el que deba recaer la acción típica así lo avala). Además, la modalidad comisiva a través de manipulaciones informáticas tiende a conseguir una transferencia no consentida de activos patrimoniales"*[102]. Y en la misma línea puede ser citado BAJO FERNANDEZ, en cuanto defiende una posición similar a la anteriormente expuesta para el tipo básico de estafa extrapolable para la estafa informática: *"así lo entiende la ley, que no considera consumado el delito de estafa hasta que no se produzca un daño patrimonial"*[103].

Entendiendo así el bien jurídico como aquel objeto de protección por el tipo penal, no ha de confundirse éste con el objeto material del delito u objeto de la acción; así, el bien jurídico protegido por el delito de estafa informática es el patrimonio, mientras que el objeto material del delito se concreta en aquella cantidad o cuantía determinada objeto de transmisión no consentida.

---

[101] ANTON ONECA, J., *"Las estafas y otros engaños, en el Código penal y la jurisprudencia", Nueva Enciclopedia Jurídica*, tomo IX, 1957, pág. 365.
[102] REY HUIDOBRO, L.F, *op.cit.*, pág. 5.
[103] BAJO FERNANDEZ, M., *Los delitos de estafa en el Código Penal*, Editorial Universitaria Ramón Areces, Madrid, 2004, pág. 22 y ss.

Pese a la expresión empleada por el artículo 248.2 del Código Penal, *"activo patrimonial",* ha de entenderse dicho patrimonio en sentido amplio[104]; así, la Real Academia Española entiende por activo el *"conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo"*.

4. Elementos de la punición

4.1 Ejecución

La estafa informática se configura como un delito de resultado, es decir, el tipo requiere para su consumación de la producción de un resultado (perjuicio patrimonial) como consecuencia de la conducta y distinto de la misma[105]; por ello, es posible la distinción de diversas fases en su ejecución. En este sentido, tienen cabida tanto la tentativa acabada como la inacabada[106]. Se dará la tentativa acabada cuando se realice el conjunto de actos ejecutivos (incluyendo, por ende, la transferencia no consentida de activo patrimonial) necesarios para la consecución del resultado, pero éste, sin embargo, no llegue a producirse, es decir, cuando no se logre ocasionar perjuicio patrimonial al sujeto pasivo. Se producirá entonces la tentativa inacabada cuando se interrumpa involuntariamente la acción delictiva sin haber realizado el sujeto activo todos los actos ejecutivos necesarios para la producción del resultado; así, por ejemplo, podrían considerarse como tentativa acabada las conductas de *phishing* en las que la víctima percibe, normalmente por fallos estructurales del mensaje o por traducciones erróneas que dejan frases carentes de sentido en el mismo, o por otro lado no tiene su cuenta en la entidad bancaria que se muestra en el mensaje no dándose por ende, ni la transferencia no consentida de activos patrimoniales ni perjuicio alguno en el sujeto pasivo.

Respecto a la consumación del tipo de estafa informática, puede extrapolarse la tesis de MESTRE DELGADO para el tipo básico de estafa, dada la similitud con la que el legislador ha construido la estructura típica de ambas figuras: *"la consumación, que acaece cuando, a la ejecución completa de la acción típica, sigue la producción del resultado prohibido por la norma, realizándose aquel concreto perjuicio*

[104] Cfr. SANCHEZ BERNAL, J., *"El bien jurídico protegido en el delito de estafa informática", Cuadernos del Tomás*, número 1, 2009, pág. 121.
[105] LUZÓN PEÑA, D.M., *op.cit.*, pág. 165.
[106] REY HUIDOBRO, L.F, *op.cit.*, pág. 8.

patrimonial"[107]; se da por ende la consumación del tipo de estafa informática una vez producido el resultado típico, es decir, el perjuicio patrimonial. Sin embargo, se ha de recalcar nuevamente la tesis expuesta, en cuanto continua exponiendo que *"para la consumación no se exige, sin embargo, que el sujeto activo, o un tercero, experimenten un correlativo incremento de sus respectivos patrimonios"*[108], lo que parece perfectamente lógico en atención a la literalidad del precepto.

Por otro lado, en virtud de lo dispuesto por el artículo 12 del Código Penal, en concreto que *"las acciones u omisiones imprudentes sólo se castigarán cuando expresamente lo disponga la Ley"*, y dada la inexistencia de un precepto que tipifique la comisión imprudente, se debe entender concurrente únicamente la comisión dolosa.

Respecto de los actos preparatorios (provocación, conspiración y proposición) en el tipo de estafa informática, ha de entenderse en base a la redacción del propio artículo 248.2 del Código Penal, cuando dispone que *"se consideran reos de estafa"* en relación con el apartado a) del mismo, aplicable el artículo 269 del Código Penal, dado que dispone que *"la provocación, la conspiración y la proposición para cometer los delitos de robo, extorsión, estafa o apropiación indebida, serán castigadas con la pena inferior en uno o dos grados a la del delito correspondiente",* entendiendo, por ende, la punibilidad de los mismos en el presente tipo.

Si bien los comportamientos recogidos por el artículo 248.2.b), relativos a la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas informáticas, no dejan de ser actos preparatorios o de participación (según los casos)[109] del tipo de estafa informático, parece el legislador buscar un adelantamiento de las barreras de protección creando un tipo mixto alternativo *"ya que se contemplan cuatro posibles conductas o modalidades comisivas, cuya ejecución individual podría dar lugar por si sola a la realización del delito en cuestión"*[110], configurándolo además como un delito de peligro, dado que éstos *"se consuman sin necesidad de lesión, con el simple peligro […] del bien jurídico, suponiendo por tanto un adelantamiento de las barreras de protección a una fase*

[107] MESTRE DELGADO, E., *"Delitos contra el patrimonio y contra el orden socioeconómico" en* LAMARCA (Coord.), *Delitos. La parte especial del Derecho Penal*, Colex, Madrid, 2015, pág. 369.
[108] *Ídem.*
[109] *Ibidem*, pág. 364.
[110] GALAN MUÑOZ, A., *"El nuevo delito del artículo 248.2 CP ¿Un adelantamiento desmedido de las barreras de protección penal del patrimonio?", Diario La Ley*, número 6037, 2004, pág. 2.

anterior a la lesión"[111]. En este sentido, GALAN MUÑOZ refleja una serie de rasgos comunes entre construcciones similares a la del artículo 248.2.c), como los artículos 270.6, 371.1 y 400 del Código Penal y, en concreto expone que *"todos estos preceptos presentan el factor común de haber sido considerados, por parte de la doctrina mayoritaria, como artículos que crean figuras delictivas eminentemente orientadas a elevar a la categoría de delitos, lo que, en realidad, no dejarían de ser sino meros actos preparatorios de los delitos a los que cada uno de ellos hacen referencia; actos que permanecerían impunes de no ser por su expresa tipificación, ya que ni siquiera podrían ser considerados como supuestos de conspiración, de proposición o de provocación"*[112].

4.2 Autoría y participación

Son de perfecta aplicación en el tipo de estafa informática los artículos 28 y 29 del Código Penal, relativos a la autoría y participación, si bien cabe destacar que se consideran autores de un delito de fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de las estafas informáticas, y no como participes de éstas, a los sujetos que realicen las conductas antes citadas y recogidas por el artículo 248.2.b). Además, existe la posibilidad, según lo previsto por el artículo 251 bis en relación con el artículo 31 bis del Código Penal, de autoría de las personas jurídicas[113].

4.3 Circunstancias

Son de aplicación al tipo de estafa informática casi todas las circunstancias atenuantes y agravantes recogidas en el Código penal; en este sentido, dada la propia redacción del artículo 22.1º del Código Penal, cuando expone que *"hay alevosía cuando el culpable comete cualquiera de los delitos contra las personas"*, se entiende la inaplicabilidad de dicha circunstancia agravante. Por otro lado, pese a que no se desprende de forma literal del propio precepto como en el caso anterior, puede entenderse de igual manera inaplicable la agravación del artículo 20.5º del Código Penal, relativa al ensañamiento, dado que difícilmente se podrá, en un delito como la estafa informática, aumentar deliberada e inhumanamente el sufrimiento de la víctima. Por otro lado, la

[111] LUZÓN PEÑA, D.M., *op.cit.*, pág. 169.
[112] GALAN MUÑOZ, A., *"El nuevo delito del artículo 248.2 CP…"*, pág. 2.
[113] MESTRE DELGADO, E., *op.cit.*, pág. 368.

circunstancia mixta de parentesco será de aplicación en virtud de lo dispuesto por el artículo 268 del Código Penal, como eximente de responsabilidad criminal siempre que no concurra violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad al ser la estafa informática un delito patrimonial. Por último, cabe la inaplicabilidad de la circunstancia recogida por el artículo 20.6º del Código Penal, relativa al abuso de confianza por la aplicación preferente del subtipo agravado del artículo 250.1.6º, aplicable cuando *"se cometa con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional*"[114].

4.4 Penalidad

Se expondrá el presente apartado, siguiendo la estructura del Código Penal y en base a la tesis aportada por MESTRE DELGADO[115], matizando determinadas cuestiones en lo relativo al delito de estafa informática. Cabe reiterar la aplicabilidad de las disposiciones relativas al tipo básico de estafa en atención a la redacción del propio artículo 248.2 del Código Penal, al considerar como reos de estafa a los sujetos que realicen las conductas descritas por el mismo.

Puede observarse, en primer lugar, la modalidad leve del delito de estafa informática en base a la cuantía de lo defraudado; en este sentido, de no superar ésta la cantidad de 400 euros, podrá imponerse pena de multa de uno a tres meses en atención a lo expuesto por el artículo 249 del Código Penal en su párrafo segundo; de superar la cuantía de lo defraudado la cantidad de 400 euros, sería de aplicación el párrafo primero del artículo 249 del Código Penal, siendo imponible una pena de prisión de seis meses a tres años.

Por otro lado, como se mencionó al comienzo del presente apartado, serán de perfecta aplicación al tipo de estafa informática las disposiciones relativas a la estafa tradicional; en este sentido, será de aplicación a la estafa informática el artículo 250 del Código Penal, concerniente a los subtipos agravados siendo en su caso imponible una pena de prisión de uno a seis años y multa de seis a doce meses cuando se produzca una de las circunstancias recogidas en el artículo 250.1 del Código Penal, y una pena de

[114] MESTRE DELGADO, E., *op.cit.*, pág. 369.
[115] *Ibidem*, págs. 369 a 371.

prisión de cuatro a ocho años y multa de doce a veinticuatro meses de concurrir la circunstancia del apartado 1º con las de los apartados 4º, 5º, 6º, 7º, o bien cuando el valor de lo defraudado superaré la cantidad de 250.000 euros en base a lo dispuesto al artículo 250.2 del Código Penal.

Como ya se ha mencionado en el apartado relativo a la autoría y participación, pueden ser responsables las personas jurídicas por estos comportamientos en atención a lo dispuesto por el artículo 251 bis en relación con el artículo 31 bis, imponiéndose bien una *"multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años"* o una *"multa del doble al cuádruple de la cantidad defraudada, en el resto de casos"*. Expone además el precepto que, *"atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33".*

En materia de concursos, cabe destacar que, pese a que pudiera pensarse en la viabilidad de un concurso medial de delitos entre la conductas de fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas informáticas del artículo 248.2.b) del Código Penal y la propia estafa informática del artículo 248.2.a), parece tal afirmación chocar con el principio *non bis in ídem;* piénsese, por ejemplo, en un sujeto que meramente adquiere, es decir, detenta o pose un programa informático que posteriormente es usado por el mismo para la comisión del tipo de estafa informática. En este sentido, las conductas tipificadas por el artículo 248.2.b) no dejan de ser en mayor o en menor medida actos preparatorios o medios comisivos del delito de estafa informática, abarcando o absorbiendo ésta la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas informáticas, pareciendo por lo tanto más viable la aplicación del artículo 8 del Código Penal para la punición de estos supuestos como un delito de estafa informática del artículo 248.2.a) del Código Penal.

Se caracteriza especialmente la estafa informática por ser una conducta dinámica, caracterizada por el automatismo inherente a los medios empleados que permiten, mediante una única instrucción, comando u orden del sujeto activo, la repetición de la conducta; es por ello que habitualmente será de aplicación lo dispuesto por el artículo 74

del Código penal en lo relativo al delito continuado, lo cual queda recogido por el artículo 74.2 del Código Penal cuando dispone que *"si se tratare de infracciones contra el patrimonio, se impondrá la pena teniendo en cuenta el perjuicio total causado. En estas infracciones el Juez o Tribunal impondrá, motivadamente, la pena superior en uno o dos grados, en la extensión que estime conveniente, si el hecho revistiere notoria gravedad y hubiere perjudicado a una generalidad de personas".* No obstante, como de forma muy precisa expone MESTRE DELGADO, en virtud del principio *non bis in ídem* no puede ser aplicada la continuidad delictiva conjuntamente a los supuestos agravados de los artículos 250.1.4º y 5º, en cuanto se tenga en cuenta para la apreciación de ambos supuestos la entidad de los perjuicios ocasionados o la situación económica en la que se deje a víctimas o familias, siendo de aplicación en esos casos de incompatibilidad, en virtud del artículo 8.1 del Código Penal (principio de especialidad), el subtipo agravado del delito de estafa informática[116].

4.5 Responsabilidad civil

Será de aplicación el título V del libro I, del Código Penal; sin embargo, pueden destacarse los artículos 109.1 del Código Penal, en cuanto dispone *que "la ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados"*, y el artículo 110 del Código Penal, relativo a la extensión de la responsabilidad civil. No debe olvidarse tampoco por su relevancia el artículo 116 del Código Penal cuando expone que *"toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que deba responder cada uno";* también que *"los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables"* y que *"la responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil en los términos establecidos en el artículo 110 de este Código de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos".*

Parece también de interés, pese a que no se exponga con detalle por cuestiones de espacio, la tesis expuesta por REY HUIDOBRO, en lo relativo a la responsabilidad civil

[116] MESTRE DELGADO, E., *op.cit.*, pág. 371.

en la estafa informática y al sujeto indemnizable, dado que realiza una interpretación de la Ley 16/2009, de 13 de noviembre, de servicios de pago, centrándose en el artículo 18 de la misma y desarrollado por la Orden EHA/1608/2010, de 14 de junio, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago, exponiendo la cuestión de quién debe ser indemnizado finalmente, si el propio titular de la cuenta bancaria, o la entidad bancaria de la que es cliente, exponiendo además los supuestos en los que dicha entidad se subrogará en la posición del cliente a efectos de percibir la responsabilidad civil de los responsables del delito tras haber cubierto al cliente la cantidad sustraída de su cuenta[117].

5. La estafa informática como delito independiente del tipo básico de estafa

Se hace necesario, previo estudio de los elementos de los tipos de estafa tradicional y de estafa informática, el posicionamiento respecto a la discusión doctrinal referente a la posibilidad de entender las defraudaciones informáticas como estafas tradicionales carentes de engaño y error, o bien por otro lado, entender que éstas gozan de una naturaleza autónoma[118] .

Parece pues, en principio, que no cabe discusión doctrinal en lo relativo a la inexistencia de los elementos engaño bastante y error en el tipo de estafa informática, siendo el propio artículo 248.2 del Código Penal el que omite la necesidad de concurrencia de engaño o error para su apreciación. Dicho precepto, pese a gozar de una estructura similar al artículo 248.1 del Código Penal, y pese a que mantiene elementos típicos comunes o excesivamente parecidos como el ánimo de lucro, el perjuicio a tercero y la necesidad de una transferencia no consentida de activo patrimonial (figura que mantiene una cierta similitud con el acto de disposición requerido en la estafa tradicional), y pareciendo, además, sustituir para un sector de la doctrina la manipulación informática o artificio semejante a los elementos engaño bastante y error, ha de entenderse como un tipo de naturaleza autónoma, tesis apoyada por autores como CONDE-PUMPIDO FERREIRO, en cuanto refiere que *"no constituye un subtipo o modalidad de estafa básica, sino un delito independiente de aquella con sus propios elementos*

[117] Vid. REY HUIDOBRO, L.F, *op.cit.*, págs. 14 y ss.
[118] CALLE RODRÍGUEZ, M.V., *"El delito de estafa informática"*, *La Ley Penal*, número 37, 2007, pag. 5.

constitutivos"[119], o ROVIRA DEL CANTO, cuando determina que *"hay que afirmar […] que se trata de «un tipo defraudatorio que no comparte la dinámica comisiva de la estafa tradicional y, en consecuencia, ajeno a la elaboración doctrinal y jurisprudencial de los elementos que la configuran» siendo la ratio legis del precepto «el criminalizar conductas lesivas para el patrimonio ajeno extramuros de la dinámica comisiva presidida por el engaño »"*[120].

Como conclusión a lo anteriormente desarrollado, puede destacarse lo dispuesto por la STS 1476/2004, de 21 de diciembre, cuando refiere que *"el tipo penal del art. 248.2 CP tiene la función de cubrir un ámbito al que no alcanzaba la definición de la estafa introducida en la reforma de 1983 […]. La nueva figura tiene la finalidad de proteger el patrimonio contra acciones que no responde al esquema típico del art. 248.1 CP, pues no se dirigen contra un sujeto que pueda ser inducido a error"*.

5.1 Elementos del tipo básico de estafa

Puede definirse la estafa como *"la conducta engañosa con ánimo de lucro injusto, propio o ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición, consecuencia del cual es un perjuicio en su patrimonio o en el de un tercero"*[121], definición que por otro lado, coincide con lo dispuesto por el artículo 248.1 del Código Penal en cuanto *"cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno".*

Junto con lo anterior, existe numerosa jurisprudencia que especifica los distintos elementos que conforman el tipo básico de estafa; así, pueden observarse las SSTS 993/2002, de 27 de mayo, 832/2014, de 12 de diciembre, y 135/2015, de 17 de febrero, siendo éstos concretamente el engaño bastante, el error, la existencia de un acto de disposición, ánimo de lucro y un perjuicio del engañado o de un tercero.

[119] CONDE-PUMPIDO FERREIRO, C., *op.cit.*, pág. 217.
[120] ROVIRA DEL CANTO, E., *op.cit.*, pág. 563.
[121] ANTON ONECA, J., *op.cit.*, pág. 365.

5.1.1 Engaño bastante o conducta engañosa

Manteniendo la línea argumental seguida con anterioridad, el primero de los elementos del tipo básico de estafa consiste en la utilización de un engaño suficiente o bastante.

Debe entenderse por engaño bastante *"aquella simulación o disimulación capaz o apta para inducir a una o varias personas a error"*[122]; sin embargo, parece correcta la matización de tal definición mediante la exposición de la postura adoptada por el Tribunal Supremo, en concreto, en la STS 135/2015, de 17 de febrero, cuando dispone que *"el engaño característico de la estafa precisa de un mínimo de idoneidad para integrar la tipicidad definida por el art. 248 CP […] «Antecedente», «causante» y «bastante» es el triple calificativo que caracteriza al engaño típico de la estafa"*; en ese mismo sentido se pronuncia también la STS 614/2016, de 8 de julio, en cuanto refiere que *"en definitiva, el engaño debe ser antecedente, causante y bastante, entendido este último en sentido subjetivo como suficiente para viciar el consentimiento del sujeto pasivo […]que las falsas maquinaciones «sean suficientes e idóneas para engañar a cualquier persona medianamente avisada». Engaño bastante que debe valorarse por tanto «intuitu personae», teniendo en cuenta que el sujeto engañado, puede ser más sugestionable por su incultura, situación, edad o déficit intelectual […] idoneidad valorada tanto atendiendo a módulos objetivos como en función de las condiciones personales del sujeto afectado y de la totalidad de circunstancias del caso concreto"*. En síntesis y a modo de conclusión, para hablar de engaño bastante e idóneo ha de lograr este el vencimiento de los mecanismos de autoprotección del sujeto pasivo, entendiendo, por lo tanto, que no será tal engaño bastante suficiente cuando dichas barreras de autoprotección hubiesen sido suficientes para vencerlo, siendo así el engaño insuficiente para la producción del perjuicio patrimonial como elemento del tipo básico de estafa[123].

[122] MATA Y MARTÍN, R.M., *Delincuencia informática….*, pág. 38.
[123] Cfr. CHOCLÁN MONTALVO, J.A., *"Engaño bastante y deberes de autoprotección"*, *Actualidad Jurídica Aranzadi*, número 398, 1999, pág.1.

5.1.2 Error

Consiste el segundo de los elementos del tipo de estafa tradicional en la situación de error producida al sujeto pasivo ocasionada mediante el empleo del primero de los elementos del tipo, el engaño bastante.

Ha de entenderse por error el conocimiento viciado de la realidad[124] o representación equivocada de un hecho[125], es decir, aquella situación de discordancia entre la representación de la realidad por parte de quien sufre el engaño y los verdaderos hechos acaecidos, provocada por el sujeto activo mediante la conducta engañosa[126], debiendo tratarse, por tanto, de la producción de "*un error, en la víctima del delito, sobre la realidad de la representación defraudatoria que recibe del sujeto activo del mismo, y especialmente respecto del significado y transcendencia económica del acto de disposición económica del acto de disposición económica que va a realizar"*[127].

Pronunciándose en el mismo sentido el Tribunal Supremo puede citarse la STS 561/2001, de 3 de abril, en cuanto refiere la necesidad de la *"producción de un error esencial en el sujeto pasivo, desconocedor o con conocimiento deformado o inexacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio del agente, lo que le lleva a actuar bajo una falsa presuposición, a emitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se produce el traspaso patrimonial".*

5.1.3 Acto de disposición

Se configura la realización del acto de disposición como el tercero de los elementos del tipo básico de estafa, deviniendo éste como consecuencia del error mencionado en el apartado anterior. Se define dicho acto por la STS 1036/2007, de 12 de diciembre, como aquel *"comportamiento de la persona inducida a error, que arrastre o conlleve de forma directa la producción de un daño patrimonial a sí misma o a un tercero,*

[124] MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 38.
[125] GARCIA VALDES, C., MESTRE DELGADO, E., FIGUEROA NAVARRO, C., *Lecciones de derecho penal parte especial*, Edisofer, Madrid, 2015, pág. 139.
[126] JAVATO MARTÍN, A.M., *"Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjeta y otros instrumentos de pago. Recensión del libro de Ricardo M. Mata y Martín"*, *Revista Electrónica de Ciencia Penal y Criminología*, número 10, 2008, pág. 2.
[127] MESTRE DELGADO, E., *op.cit.*, pág. 363.

no siendo necesario que concurran en una misma persona la condición de engañado y de perjudicado".

Aborda en relación a lo anterior la STS 476/2009, de 7 de mayo, la cuestión relativa a la posible apreciación de voluntariedad en la realización del acto dispositivo, y aclara que *"en el caso de la estafa no cabe imputar a la víctima el desapoderamiento que resulta, cuando no actúa voluntariamente. Y no cabe hablar de voluntariedad, en ese sentido, aun cuando el acto de desplazamiento sea voluntario, si esa voluntad es fruto del engaño"*. Puede, además, afectar dicho acto de disposición a cualquier elemento patrimonial; así, por ejemplo, la entrega de cosa material o cantidad dineraria, actos de disposición en documento público o privado, prestación de servicios susceptibles de una valoración económica entre otros.

5.1.4 Ánimo de lucro

Se configura el ánimo de lucro como el cuarto elemento configurador del tipo básico de estafa, el cual ha de entenderse, en base a lo dispuesto por la STS 187/2002, de 8 de febrero, como aquel *"elemento subjetivo del injusto, exigido hoy de manera explícita por el artículo 248 del CP entendido como propósito por parte del infractor de obtención de una ventaja patrimonial correlativa, aunque no necesariamente equivalente, al perjuicio típico ocasionado, eliminándose, pues, la incriminación a título de imprudencia";* y, en el mismo sentido que la anterior, recoge la STS 1232/2002, de 2 de julio, una concepción de ánimo de lucro como aquel *"elemento subjetivo del injusto o dolo en el sujeto activo de la acción, según la jurisprudencia y la doctrina aparece integrado por el elemento «intelectivo» de «conocer que se está engañando y perjudicando a otro» y el «volitivo» de obtener una ventaja o provecho, es decir, la propia norma al definir el tipo delictivo exige expresamente el «ánimo de lucro» u obtención de un provecho económico como contrapartida al perjuicio a que antes nos hemos referido"*.

Con el paso del tiempo la jurisprudencia ha flexibilizado de forma considerable la concepción del ánimo de lucro, considerando como tal cualquier tipo de utilidad, satisfacción o aprovechamiento obtenido por la realización del hecho; en este sentido, y con la finalidad de ejemplificar lo anterior, debe citarse de nuevo la STS 1232/2002, de 2 de julio, en cuanto dispone que *"una vez detectada la existencia de un engaño*

antecedente y de un perjuicio consiguiente para las víctimas o sujetos pasivos de la acción, resulta clara la concurrencia de este elemento típico del ánimo de lucro, porque, en definitiva, este ánimo se centra «en el propio acto dispositivo provocado por el engaño» y va ínsito en el carácter patrimonial de la ventaja que se pretende obtener aunque no es imprescindible que se concrete exclusivamente en el valor económico de la casa, ya que, como ha expuesto la doctrina y recoge la jurisprudencia, «el lucro se utiliza en estos delitos con un sentido jurídico de cualquier clase de utilidad o ventaja»".

Por último, el ánimo de lucro puede ser en beneficio propio o de un tercero y en ese mismo sentido se expresa la STS 377/2016, de 3 de mayo, cuando dispone que *"no se desmoronaría la tipicidad de la estafa que como pone bien de manifiesto el Fiscal no exige que el lucro sea propio; puede ser un lucro ajeno"*.

5.1.5 Perjuicio del engañado o de tercero

Como quinto y último elemento configurador del tipo de estafa tradicional, se encuentra el perjuicio del engañado o de tercero, siendo éste el verdadero resultado del delito y debiendo darse este con posterioridad a la conducta engañosa del sujeto activo. Dado el carácter de resultado del tipo que mantiene este elemento, se entiende de necesaria concurrencia para la apreciación de consumación del delito[128], funcionando, además, como elemento cuantitativo determinante para la posible aplicabilidad del artículo 249 párrafo 2º del Código Penal, que permite hablar de delito leve de estafa siempre que la cuantía del perjuicio no sea superior a los 400 euros.

Reafirmando lo ya expuesto se expresa la STS 1232/2002, de 2 de julio, en cuanto, *"además de la existencia de un engaño bastante y de que exista una relación de causalidad entre ese engaño y el error producido en el sujeto pasivo de la acción, el tipo delictivo de la estafa requiere como requisito ineludible para que pueda consumarse la existencia de un perjuicio económico en el engañado".*

5.2 Elementos del tipo de la estafa informática

A modo de introducción, parece plasmar perfectamente los diversos elementos del tipo, así como la relación entre ellos, la STS 692/2006, de 26 de junio. Así, *"como en la*

[128] MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 39.

estafa debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida".

5.2.1 Manipulación informática o artificio semejante

Previo análisis de la fórmula "manipulación informática o artificio semejante", parece cuanto menos necesaria la distinción entre este elemento típico y los elementos engaño bastante y error de la estafa tradicional, dado que, como se expuso en apartados anteriores, parte de la doctrina entiende que la estafa informática no deja de ser un subtipo o modalidad de estafa tradicional.

Gira el tipo básico de estafa alrededor del elemento nuclear del engaño bastante, pero cabe cuestionarse respecto a la estafa informática si, primero, es posible engañar a una máquina y segundo, si la máquina de poder ser engañada pudiese llegar a cometer un error. Parece obvio que no puede una maquina ser engañada, en el sentido del propio termino, puesto que, como bien define la Real Academia Española, se entiende por engaño el "*hacer creer a alguien que algo falso es verdadero*", pudiendo deducirse que el engaño es algo humano y que, por tanto, no puede ser entendido en una máquina, máxime cuando ésta se limita a cumplir las instrucciones, comandos u órdenes[129] dadas por el operador de forma directa o en remoto. Parece obvio, entonces, que la maquina no podrá incurrir en error, sino que se limitará a ejecutar una serie de comandos perjudiciales para el sujeto pasivo[130]. En este mismo sentido expresa el Tribunal Supremo en diversas resoluciones; así pueden apreciarse la STS de 19 de abril de 1991, cuando expone que *"con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa";* también la STS 185/2006, de 24 de febrero, cuando refiere que *"sólo puede ser engañada una persona que, a su vez, pueda incurrir en error. Por lo tanto, ni*

[129] Cfr. MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 43.
[130] Cfr. JAÉN VALLEJO, M., PERRINO PÉREZ, A.L., *La reforma penal de 2015 análisis de las principales reformas introducidas en el Código Penal por las Leyes Orgánicas 1 y 2/2015 de 30 de marzo*, Dykinson, Madrid, 2015, págs. 100 y ss.

las máquinas pueden ser engañadas […] ni el cajero automático ha incurrido en error"; y, por último, la STS 1476/2004, de 21 de diciembre, cuando señala que *"en efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, sin «error». De manera que el sujeto pasivo sólo puede ser el titular del patrimonio perjudicado".*

Dispone, como ya vimos, el artículo 248.2.a) del Código Penal que serán considerados como reos de estafa informática los que *"con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"*. Expone así el precepto antes mencionado el elemento nuclear del tipo como *"manipulación informática o artificio semejante";* sin embargo, ambos términos han de ser analizados de forma separada para su mejor entendimiento.

A) Manipulación informática

Se produce, a diferencia del tipo tradicional de estafa, una excesiva apertura o escasa delimitación de la acción típica, implicando ello la aparición de numerosas interpretaciones y pareciendo aún más amplia dicha acción típica cuando entra en escena la manipulación informática en conjunto con la expresión *"o artificio semejante"*. Parece, con ello, que el legislador pretende evitar cualquier tipo de laguna legal derivada de la celeridad de desarrollo tecnológico y del gran potencial delictivo que pudieran adquirir en un futuro estas conductas al albur del mismo.

Sin embargo, pese a la amplitud conceptual antes descrita, determinados autores realizan una interpretación del mismo mediante el artículo 3 de la Decisión Marco 2001/413/JAI del Consejo, entendiendo como manipulación informática *"la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o la interferencia indebida en el funcionamiento de un programa o sistema informáticos"*, siendo además dicha interpretación del termino coincidente con la realizada por el Convenio de Budapest de 23 de noviembre de 2001 sobre la ciberdelincuencia, exponiendo en su artículo 8 que *"cualquier introducción, alteración, borrado o supresión de datos informáticos; cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de*

obtener ilegítimamente un beneficio económico para uno mismo o para otra persona" [131].

Otros autores[132], sin embargo, realizan una interpretación más ajustada a la jurisprudencia existente; así, la STS 2175/2001, de 20 de noviembre, entiende la manipulación informática cuando *"la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos"* y, en el mismo sentido que aquélla, las SSTS 692/2006, de 26 de junio, 369/2007, de 9 de mayo, 860/2008, de 17 de diciembre y 539/2015, de 1 de octubre de 2015.

Mientras que diversos autores buscan la delimitación de este concepto tan amplio, mediante diversos métodos, otros como FERNANDEZ TERUELO proponen alternativas para la modificación del mismo; por ejemplo, el autor antes mencionado propone el cambio de la expresión "manipulación informática o artificio semejante" por la fórmula "operaciones informáticas no autorizadas", motivando tal cambio en la inadecuada cobertura que, según su criterio, mantiene el actual tipo para conductas relacionadas con el uso de *dialers* o el *spyware*[133]. Sin embargo, dicha amplitud conceptual no deviene quizá tanto de la expresión manipulación informática como de la fórmula que la acompaña ("o artificio semejante") que, como ya se analizará en su momento, podría chocar con los principios de legalidad y seguridad jurídica, al no permitir una correcta delimitación de las conductas que podrían subsumirse en la misma.

Puede la ya referida manipulación informática, dada su amplitud conceptual, producirse de formas muy diversas, ya sea en el mismo programa o bien en cualquier momento del procesamiento o tratamiento automatizado de datos, pudiendo darse, tanto durante la entrada como durante la salida de estos, permitiendo además el medio informático la producción de la manipulación, no necesariamente en presencia física del dispositivo afectado, sino desde cualquier lugar.

Pueden, así, clasificarse las manipulaciones informáticas, en atención a las cualidades o circunstancias que rodean al sujeto activo, en manipulaciones internas y externas. Se entiende, pues, en relación al sujeto activo como manipulación interna, aquella en la que éste se encuentra autorizado para el acceso a la plataforma informática

[131] DE LA MATA BARRANCO, N.J, HERNANDEZ DIAZ, L., *op.cit.*, págs.183 y ss.
[132] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 48.
[133] *Ibidem*, pág. 52.

y a su sistema; en contraposición, constituirá la manipulación externa, aquella manipulación llevada a cabo por un sujeto ajeno y, por tanto, no autorizado por la persona o entidad de la que depende tal plataforma, siendo así cualquier acceso a ella ilegítimo. Expone MATA Y MARTÍN la existencia de dos criterios de clasificación de las manipulaciones como interiores o exteriores, el ya mencionado, y otro, en atención al lugar desde el cual accede el sujeto activo a la plataforma, entendiendo como manipulación interna aquella que se desarrolla dentro de un marco de cercanía o acceso directo a la plataforma; puede ponerse como ejemplo, al propio ordenador o *smartphone* objeto de la manipulación, y externa cuando se produce un acceso en remoto a una cierta distancia mediante internet[134]. Pues bien, ha de entenderse algo anticuado tal criterio clasificatorio puesto que abundan hoy los programas que permiten el acceso remoto autorizado a distintos dispositivos mediante la introducción de una misma clave en ambos; así por ejemplo aplicaciones como *teamviewer* permiten el acceso y control remoto entre ordenadores. Se desprende en síntesis de la anterior afirmación que, pese a que pueda realizarse una clasificación de las diversas formas de manipulación, no cabe realizar una absorción en un mismo criterio clasificatorio de diversas conductas, obviando, por ejemplo, el hecho de que un acceso remoto implique de por sí un acceso no autorizado. Se requiere, por tanto, siendo ello una mera opinión susceptible de discusión, de una nueva serie de criterios clasificatorios, proponiéndose en este sentido el mantenimiento de los criterios de manipulación interior y exterior en atención al sujeto activo, y la creación de otro tipo de calificación según el lugar en el que se acceda, proponiendo criterios como manipulación a distancia y manipulación directa.

Pueden también clasificarse las manipulaciones informáticas en activas u omisivas, y si bien la primera de ellas no supone un tema controvertido, ello sí es así para el segundo caso, existiendo una cierta divergencia hacia la aceptación o no de los supuestos de manipulación omisiva. Así, autores como ROVIRA DEL CANTO[135] entienden la imposibilidad de comisión por omisión en el tipo de estafa informática, exponiendo el autor: *"no considero factible por lo expuesto la posibilidad de su realización omisiva, y de muy difícil configuración, por no decir imposible, su comisión por omisión*. En contraposición a este autor tanto MATA Y MARTÍN cuando expone que *"si admitimos como manipulación, como se hace muy habitualmente, el supuesto de no*

[134] MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 50.
[135] ROVIRA DEL CANTO, E., *op.cit.*, pág. 576.

inclusión de los datos reales que deberían ser objeto de procesamiento […] lo que hemos llamado manipulación previa, estamos abarcando la omisión"[136], como FARALDO CABANA cuando expone que *"se plantea la duda relativa a si constituye manipulación no introducir datos que deberían haber sido procesados. Al igual que en la estafa común, en la mayoría de los supuestos nos encontramos ante omisiones que tienen lugar en el marco de actos concluyentes de carácter positivo, por lo que no resulta problemático incluirla"*[137], defienden la posibilidad de comisión omisiva de la manipulación informática. Se procederá en el presente trabajo al apoyo de la segunda de las tesis expuestas, primero, dado que se mantiene, como se verá a continuación, la tesis respectiva a la clasificación como manipulación previa, de programa y posterior, siendo por ello el mantenimiento de la primera de las tesis, del todo incongruente, y segundo, porque parece perfectamente viable la comisión por omisión de la manipulación informática en cuanto la no introducción de datos sobre los que operara el programa produciría una alteración del resultado que, de forma normal, se habría obtenido de introducir los datos correspondientes. Si bien es cierto que la admisibilidad de supuestos omisivos entraña cierta dificultad en su apreciación, dado que las conductas, en principio omisivas pueden ser reconducidas a actos concluyentes como bien exponen VALLE MUÑIZ y FARALDO CABANA, autores que parece adoptar una posición muy similar a la STS 621/2014, de 23 de septiembre, relativa al tipo básico de estafa extrapolable a la estafa informática; sin embargo, en numerosas ocasiones, los comportamientos que en un principio se tienen por omisivos y que, parecen de una admisibilidad dudosa, son en realidad comportamientos activos en *strictu sensu*[138].

Visto lo anterior, existen además criterios clasificatorios que requieren un cierto grado de conocimientos técnicos; sin embargo, no se ocupará el presente trabajo de ellos con excesivo detalle, baste completar lo dispuesto en el párrafo anterior con una breve exposición de otros criterios clasificatorios de las manipulaciones. Existen pues, y en ello coinciden autores como GUTIÉRREZ FRANCÉS[139] o MATA Y MARTÍN[140], manipulaciones previas producidas en fase de *input*, que implican la actuación durante la entrada de datos sobre los que actúa el programa siendo así, por ejemplo, la introducción

[136] MATA Y MARTÍN, R.M., Delincuencia informática…., págs. 54 y ss.
[137] FARALDO CABANA, P., *"Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática", Eguzkilore*, número 21, 2007, págs. 43 y ss.
[138] Cfr. MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 54.
[139] Cfr. GUTIERREZ FRANCES, M.L., *op.cit.*, pág. 116 y ss.
[140] Cfr. MATA Y MARTÍN, R.M., *Delincuencia informática….,* págs. 50 y ss.

o adición de datos falsos, modificación de datos existentes o supresión u omisión de datos durante el registro de los mismos, pueden darse también manipulaciones del programa, que implicarían una modificación de las instrucciones o programación, es decir, en la introducción de nuevas órdenes, alterar o suprimir las ya existentes en el código fuente, y por último, podemos hablar de manipulaciones posteriores, producidas durante la salida de datos, en las que se produce una alteración no ya en los datos previos o sobre el propio programa, sino sobre la exteriorización del resultado del procesamiento al exterior, siendo así, por ejemplo, una visión distorsionada al ser visualizado el resultado en la pantalla, durante la impresión en papel o durante la transmisión de datos a chips de tecnología NFC (comunicación de campo cercano), registros de banda magnética, entre otras posibles.

Conviene enfatizar, a modo de conclusión, la necesidad de una correcta interpretación conceptual de la manipulación informática, puesto que se requiere, para la realización del tipo, de una manipulación informática *strictu sensu*, es decir, en el caso de una utilización de la plataforma informática, como medio auxiliar o de ayuda del sujeto activo para inducir al sujeto pasivo a la toma de decisiones no puede considerarse manipulación informática, sino como un engaño y, por ende, habrían de calificarse así dentro del tipo básico de estafa del artículo 248.1 del Código Penal.

B) Artificio semejante

Parece el legislador, con la cláusula "o artificio semejante", querer evitar futuras situaciones de laguna legal derivadas de la velocidad con la que se producen los nuevos avances tecnológicos, abriéndose con ellos nuevas posibilidades delictivas.

Se muestra un término extenso que, en un primer momento, podría parecer incierto e indeterminado y, por ello, contrario al principio de taxatividad y de un dudoso encaje dentro los principios de legalidad y de seguridad jurídica. Sin embargo, ello no es así; ha de realizarse, en este sentido, pese a la gran amplitud conceptual de la cláusula "o artificio semejante", una interpretación algo restrictiva en aras de concretar qué conductas serán abarcables por dicho término. Como bien expone MATA Y MARTÍN, se requiere de una semejanza del artificio a la manipulación informática[141], no pudiendo aunar bajo *"artificio semejante"* cualquier tipo de conducta, sino solo aquellas que mantengan una

[141] MATA Y MARTÍN, R.M., *Delincuencia informática….,* pág. 48.

estrecha relación con la informática[142]. Parece además así quererlo el legislador en cuanto la propia etimología de la palabra empleada en el precepto *"semejante"* implica, según la Real Academia Española *"que semeja o se parece a alguien o algo"*, por ende, podemos concluir que serán los artificios informáticos semejantes los incluidos en el tipo del artículo 248.2 del Código Penal, excluyendo así los artificios no informáticos[143].

Puede reafirmarse lo anterior mediante lo expuesto por la STS 1476/2004, de 21 de diciembre: *"lo importante es, ante todo, la realización de las acciones constitutivas de un artificio semejante a una manipulación informática. En efecto, al texto del art. 248.2 CP considera aplicable la pena de la estafa cuando el autor se ha valido de «alguna manipulación informática» o de algún «artificio semejante». La cuestión de cuáles son los artificios semejantes debe ser determinada por la aptitud del medio informático empleado para producir el daño patrimonial"* y en el mismo sentido que la anterior, las SSTS 369/2007, de 9 de mayo, y 860/2008, de 17 de diciembre, en cuanto reiteran la idea plasmada por la anterior. Es apreciable así la necesidad de una relación del artificio primero, con la informática, y segundo, con la manipulación informática propiamente dicha para su subsunción dentro del tipo del artículo 248.2.a) del Código Penal.

5.2.2 Transferencias no consentidas de activo patrimonial

Se requiere, en primer lugar, para hablar de un supuesto de estafa informática, de la justificación de existencia de nexo causal entre la manipulación informática o artificio semejante con la transferencia no consentida de activo patrimonial, funcionando así tal manipulación o artificio como una *conditio sine qua non* para hablar de un delito de estafa informática; en este sentido, parece muy esclarecedora la STS 692/2006, de 26 de junio, que expone *"cómo en la estafa debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida"*.

Se presenta entonces la transferencia no consentida de activo patrimonial con una cierta similitud a los actos de disposición del tipo básico de estafa que fue analizado con anterioridad; sin embargo, a diferencia de estos actos, en la estafa informática se produce

[142] Cfr. FARALDO CABANA, P., *"Los conceptos de manipulación informática…"*, pág. 43.
[143] Cfr. GALAN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P*, Tirant lo Blanch, Valencia, 2005, págs. 566 y ss.

dicha transferencia sin necesidad de concurrencia de engaño ni error en la persona, requiriéndose, sin embargo, la existencia de una manipulación informática o de un artificio semejante desencadenante la misma. No obstante, no han de confundirse ambos conceptos puesto que, como ya se pudo analizar, el acto de disposición consistía en un comportamiento realizado por el sujeto pasivo movido o inducido por el engaño bastante, previo a tal acto dispositivo que arrastraba consigo la producción de un daño patrimonial para sí o un tercero, difiriendo así de la transferencia no consentida de activo patrimonial en cuanto ésta no ha sido realizada voluntariamente por el sujeto pasivo objeto de la estafa informática y debiéndose tal desplazamiento patrimonial a la realización de una manipulación informática o artificio semejante por el sujeto activo.

Supone así la transferencia un desplazamiento patrimonial, no consentido por el sujeto pasivo que ha sufrido de la manipulación informática o artificio semejante, llegando a ser, en determinadas ocasiones, desconocida por el sujeto hasta pasado cierto tiempo; a modo de ejemplo, pudiera pensarse en un sujeto que desconoce dicha transferencia hasta el momento en el que consulta el estado de su cuenta bancaria y descubre una retirada de fondos desconocida.

En cuanto a la forma en la que se puede realizar la transferencia no consentida de activo patrimonial, ha de mencionarse la STS 2175/2001, de 20 de noviembre, y en relación y apoyo a la misma las SSTS 692/2006, de 26 de junio, y 860/2008, de 17 de diciembre, en cuanto exponen que el propio artículo 248.2 del Código Penal *"permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia"*. En este mismo sentido se expresa CALLE RODRIGUEZ acertadamente refiriendo que el artículo 248.2 del Código Penal *"castiga, únicamente, las transferencias electrónicas de fondos, sin comprender las conductas que no provoquen una operación de este tipo. No son incluibles aquí, por tanto, sino en la modalidad delictiva que corresponda en cada caso, las manipulaciones que se dirijan a encubrir apoderamientos o disposiciones efectuadas por otros medios (por ejemplo, modificar inventarios para ocultar la sustracción de materiales, alterar la contabilidad para encubrir desfalcos, etc.)"*. Entiende así la RAE el término "activo" como el *"conjunto de bienes y derechos con*

valor monetario que son propiedad de una empresa, institución o individuo", y el de "transferir" como el *"pasar o llevar algo desde un lugar a otro"*, lo que concuerda con lo descrito anteriormente, y entiende así por todo ello la autora que las transferencias no consentidas de activo patrimonial consisten en un proceso meramente contable (cargar débitos, descontar activos, ordenar anotaciones a favor de otro sujeto, entre otras) o la realización de determinadas prestaciones o servicios a su favor (cargo de títulos o billetes de transporte a favor de terceros, falsas órdenes de pago, entre otras)[144]. Por último, se requiere que esta transferencia patrimonial no sea consentida, dado que, de mediar consentimiento del sujeto pasivo, el hecho no podría calificarse como un delito de estafa informática del artículo 248.2 del Código Penal[145].

5.2.3 Ánimo de lucro

Baste, para la exposición del presente apartado, la remisión a lo dispuesto para el tipo de estafa tradicional, en tanto es perfectamente extrapolable para la estafa informática.

5.2.4 Perjuicio patrimonial

Hemos de entender como perjuicio patrimonial, en el sentido del texto del artículo 248.2 del Código Penal, aquel perjuicio que se produce a raíz de una manipulación informática o artificio semejante sobre una plataforma informática, pudiendo ello completarse por la STS 369/2007, de 9 de mayo, en cuanto refiere que *"con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa",* pudiendo así excluir la tipicidad, dentro de la estafa informática, de aquellos supuestos en los que el perjuicio no es producido por dicha manipulación informática o artificio semejante y entendiendo que se produce la materialización o concreción del daño en una transferencia no consentida de activo patrimonial. Así, puede apoyarse lo anterior mediante la cita de la

[144] CALLE RODRIGUEZ, M.V., *op.cit.*, pág. 9.
[145] *Ibidem*, pág. 10.

STS 2175/2001, de 20 de noviembre, cuando manifiesta que *"el perjuicio de tercero que se concreta en una transferencia no consentida"*.

Actúa, además, y es quizá su rasgo más relevante, el elemento perjuicio patrimonial como aquel que determina el grado de ejecución del tipo de estafa informática del artículo 248.2 del Código Penal, afirmación apoyada por CALLE RODRIGUEZ cuando expone que *"la consumación se alcanza cuando se produce el perjuicio, lo que coincidirá con la realización del asiento contable, por lo que es posible la tentativa"*[146] , cuestión que ya fue objeto de análisis en el presente trabajo.

5.3 Utilización ilegítima de tarjetas de crédito o débito, cheques de viaje o datos obrantes en ellos

Parece el legislador tras la reforma del Código Penal introducida por la Ley Orgánica 5/2010, querer poner fin al debate doctrinal[147] respecto a esta cuestión; en concreto, se vuelve a producir una división del artículo 248 del Código Penal en dos apartados, tal como se encontraba antes de la reforma introducida por la Ley Orgánica 15/2013, con la salvedad de que se introducen en su segundo apartado tres supuestos, centrándonos en concreto en el artículo 248.2.c) en cuanto recoge que tendrán la consideración como reos de estafa *"los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"*.

Así, como ya se adelantó, previa reforma introducida por la Ley Orgánica 5/2010, existía cierto debate doctrinal y jurisprudencial en cuanto a la calificación de estas conductas[148]; así, según las distintas circunstancias y casos concretos, se proponía dar solución al problema calificando estas conductas como hurtos[149], robos con fuerza en las cosas[150] o estafas informáticas[151][152], si bien, como señala AZCONA ALBARRÁN, *"las*

[146]CALLE RODRIGUEZ, M.V, *op.cit.*, pág. 10.
[147] FARALDO CABANA, P., *"Los delitos contra el patrimonio tras la reforma de 2010", La Ley Penal*, número 81, 2011, pág. 8.
[148] BENITEZ ORTÚZAR, I.F., *"Informática y delito. Aspectos penales relacionados con las nuevas tecnologías"* en *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, Dykinson, Madrid, 2009, pág. 131.
[149] BOLEA BARDÓN, C., ROBLES PLANAS, R*., "La utilización de tarjetas ajenas en cajeros automáticos: ¿Robo, hurto o estafa?", Diario La Ley*, tomo 4, 2011, págs. 5 y ss.
[150] *Ídem.*
[151] MUÑOZ CONDE, F., *Derecho penal. Parte especial*, Tirant lo Blanch, México D.F., 2014, pág. 374.
[152] CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch, Barcelona, 2000, pág. 309.

soluciones más generalizadas eran las que entendían que, ora se trataba de un delito de robo con fuerza en las cosas, por empleo de llaves falsas, ora nos hallábamos ante un delito de estafa (básicamente en su modalidad de estafa informática del art. 248.2 CP)"[153].

Tras la ya citada reforma introducida por la Ley Orgánica 5/2010, parece resuelta la controversia doctrinal y jurisprudencial relativa a la calificación de estas conductas como robo, hurto o estafa informática, encontrándose tales conductas tipificadas por el artículo 248.2.c); sin embargo, la introducción de dicho precepto no está tampoco exenta de polémica. Autores como BENITEZ ORTÚZAR se postulan a favor de la introducción de éste sin exponer la necesidad de ningún tipo de modificación en la redacción del tipo[154], mientras que otros autores, como FARALDO CABANA, se posicionan a favor de la necesidad de modificación del mismo por entender que deja fuera de su redacción determinadas conductas. Pone en relieve así la autora una serie de nuevos problemas y más concretamente expone que "*desde la delimitación de lo que se entiende por tarjeta de crédito o débito (¿sólo se incluyen las emitidas por instituciones financieras o también las tarjetas de cliente, emitidas por establecimientos comerciales, que sirven como instrumento de pago? ¿Qué ocurre con las tarjetas prepago o las de telepeaje, que no son ni de crédito ni de débito?), hasta la determinación de qué significa realizar operaciones de cualquier clase, pasando por la naturaleza del perjuicio causado al titular (¿sólo es el económico o puede ser de otra naturaleza? ¿Hay perjuicio cuando una entidad aseguradora se hace cargo del importe de lo defraudado?) y los efectos del consentimiento del titular a la realización de la operación (pues no se dice que la utilización no haya de ser consentida por el titular)"*[155], poniendo en manifiesto la necesidad de una nueva reformulación del tipo.

[153] AZCONA ALBARRÁN, C.D., *Tarjetas de pago y derecho penal. Un modelo interpretativo del art. 248.2.c) CP*, Atelier, Barcelona, 2012, pág. 150.
[154] BENITEZ ORTÚZAR, I.F., *op.cit.*, pág. 129.
[155] FARALDO CABANA, P., *"Los delitos contra el patrimonio…",* pág. 9.

6. Formulas específicas de fraude informático

6.1 Obtención de claves o datos de acceso y uso fraudulento de los mismos

6.1.1 Sin conocimiento de la víctima

En la actualidad, se produce dicha obtención de datos o claves de acceso sin conocimiento de la víctima mediante el *spyware*, utilizándose tal término para definir aquella conducta caracterizada por la monitorización remota mediante el uso de aplicaciones (*Browser Helper Objet*s, *Keyloggers*, entre otros) diseñadas para funcionar en el dispositivo informatizado reportando a un tercero, normalmente mediante internet, determinados aspectos sobre el dispositivo del usuario[156].

Como se vio con anterioridad, son diversas las modalidades de spyware existentes; sin embargo, no conviene en el presente trabajo realizar una exposición demasiado detallada respecto a ello, baste decir, que dentro de la amplia tipología de spyware quizá los más utilizados son los *Browser Helper Objets*, que consisten en complementos para el navegador, y los *Keyloggers* que consisten en programas que recogen las pulsaciones realizadas por el usuario y que serán posteriormente aunadas para su envió a un tercero.

La problemática surge entonces cuando se procede a introducir datos sensibles para el usuario, es decir, datos de acceso o claves que puedan producir un perjuicio a éste, como por ejemplo, pudieran ser los datos de la tarjeta de crédito (número de tarjeta, fecha de caducidad y código de seguridad) o también datos de cuenta de servicios bancarios o de pago como *PayPal* una empresa americana que permite un sistema de pagos en línea, entre otra mucha información que podría llegar a obtenerse. Dichos datos sensibles obtenidos por el sujeto activo defraudador serán, en general, utilizados por el mismo para la realización de transferencias de capital a su favor, la realización de compras en perjuicio del sujeto pasivo, entre otras conductas posibles.

[156] Cfr. QUIGLEY, M., *Encyclopedia of information ethics and security*, Information Science Reference, Hershey, 2008, pág. 616.

6.1.2 Proporcionados por la propia víctima, que, sin saberlo, hace llegar claves y datos al propio defraudador

Se produce, como en el apartado anterior, sin conocimiento de la víctima, una transmisión de datos al sujeto activo defraudador; no obstante, se produce en este caso dicha comunicación o trasmisión de aquellos datos sensibles susceptibles de ser utilizados en su perjuicio patrimonial por el propio sujeto pasivo.

Podemos destacar así, en primer lugar, la figura del *phishing,* la cual consiste por lo general en él envió de correos electrónicos a través de la técnica del *spam* (envío de correos masivo) camuflados bajo la apariencia de una fuente conocida por la víctima, siendo normalmente dichas fuentes entidades bancarias o cuentas de empresas de pagos en línea. Al amparo de la imagen de la empresa en cuestión, y asimilándose las formas del correo electrónico a las habitualmente utilizada por la empresa con sus logotipos, tipo de letra, mismo espaciado, se suelen introducir enlaces que redirigen a la víctima hacia un sitio web distinto al de entidad en el que se le solicitaran determinados datos sensibles como contraseñas, datos de la tarjeta de crédito, nombre de usuario, entre otros muchos datos a solicitar, apercibiendo o amedrentando al sujeto pasivo con fórmulas como "de no actualizar su información podría perder su cuenta o podría ser bloqueada", poniendo así, el sujeto pasivo sin saberlo, en manos del defraudador dicha información que será utilizada con sus fines delictivos[157].

Cabe concluir que, para que la conducta del *phishing* pueda calificarse como una estafa informática del artículo 248.2 del Código Penal, no basta con la mera obtención de datos sensibles, sino que dichos datos, han de servir al sujeto activo defraudador para el uso de éstos con el fin de realizar una transferencia de activo patrimonial susceptible de provocar un perjuicio patrimonial en la víctima, no encajando dentro de tal tipo como vimos la mera sustracción de datos, siendo en principio ya indiferente en aras de calificar la conducta dentro del tipo la producción de un perjuicio, puesto que como también pudimos analizar en anteriores epígrafes, funciona el perjuicio como aquel elemento determinante de la consumación. Parece además de interés citar un ejemplo en aras de esclarecer la verdadera magnitud que alcanza este tipo de conductas caracterizadas por el automatismo; así, si un mensaje *"se envía por correo electrónico a digamos 5 millones*

[157] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 29.

de personas, un 10% de las mismas que tiene una cuenta en ese Banco y 1% se acuerda de la clave y contesta, son 5.000 claves y con esas claves el hacker u otro ordena una transferencia desde la cuenta del cliente perjudicado a la del «mula o mulero». Sólo que a cada una le quitemos «solo» 1.000 euros de cada cuenta son 5 millones de euros, incluso si le sacamos a cada uno 400 euros serían 2 millones de euros"[158], puede completarse el citado ejemplo con lo ya expuesto en lo respectivo a la necesidad de una escasa inversión para la obtención de un alto beneficio, dado que en principio con una inversión inicial realmente baja (precio de un dispositivo con conexión a internet), pueden obtenerse millones de euros.

En segundo lugar, puede observarse la figura del *smishing*, una variante del *phishing y* si bien la anterior, consistía como vimos, en una estafa dentro del ámbito del correo electrónico, consiste el *smishing* en el envío de mensajes de texto de forma masiva (lo cual suele denominarse habitualmente como *spam*) por el sujeto activo o defraudador en los que se solicita información sensible del sujeto camuflándose el mensaje, como si de un caballo de Troya se tratase, detrás de una compañía de confianza, uno de nuestros contactos, o bien, como viene siendo habitual incitando al sujeto pasivo a introducir sus datos mediante la falsa creencia de que recibirá una herencia, un premio o algún vehículo o bien material por motivos diversos.

En tercer y último lugar, se puede hablar de una variante del *phishing* denominada *pharming*. A diferencia del *phishing*, en el que se utilizaba el correo electrónico como medio o soporte material para la posterior redirección de la víctima a una página web falsa, se produce en el *pharming* la instalación de un *malware* concreto dentro del servidor de internet (Google Chrome, Mozilla Firefox, entre otros), siendo tal *malware* y no el propio usuario, como ocurría con el *phishing*, el que produce una redirección de la víctima a una web falsa en la que se procederá a la obtención de datos sensibles por el sujeto activo defraudador[159].

Una vez obtenidos los datos por el defraudador mediante cualquiera de los métodos antes descritos, suelen darse dos situaciones: es habitual, en primer lugar, que el sujeto defraudador opte por abrir simultáneamente una o varias cuentas bancarias situadas

[158] CABEDO VILLAMÓN, F., ORTIZ NAVARRO, J.F., AGUADO LÓPEZ, S., *"Conductas típicas y prueba electrónica en los fraudes electrónicos" en Fraude electrónico. Panorama actual y medios jurídicos para combatirlo*, Civitas, Navarra, 2013, pág. 270.
[159] Cfr. OXMAN, N., *"Estafas informáticas a través de internet: acerca de la imputación penal del «phishing» y del «pharming»", Revista de derecho*, número 41, pág. 216.

en terceros países para así transferir a dicha cuenta el activo patrimonial estafado para un posterior cobro en tales países de una forma sencilla tendiendo a la creación de cuantas en entidades cercanas, dentro de un espacio geográfico relativamente pequeño para una mayor celeridad a la hora de retirar el capital[160], y, en segundo lugar, es también habitual la utilización de *money-mules,* es decir, "mulas" o "muleros"; estos sujetos ponen a disposición del defraudador o *scrammer* sus cuentas para que éste ingrese en ellas las cantidades defraudadas percibiendo a cambio una comisión. Además, sirven estos "muleros" como blanqueadores de las cantidades defraudadas en territorio nacional, siendo enviadas posteriormente a terceros países mediante servicios de mensajería, de empresas de envío de fondos al extranjero, como, por ejemplo, los locutorios, entre otras posibilidades[161].

Existe, como expone GOMEZ INIESTA, cierta dicotomía respecto a la posible calificación de la conducta descrita con anterioridad; existen autores que entienden la conducta de las "mulas" como una conducta típica del artículo 298.1 del Código Penal relativo a la receptación. Así, expone el precepto que *"el que, con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, en el que no haya intervenido ni como autor ni como cómplice, ayude a los responsables a aprovecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos, será castigado con la pena de prisión de seis meses a dos años"*; ello se fundamenta por dichos autores en la no participación o intervención del mulero en el delito de previo de estafa informática ni como autor ni como participe, en cuanto el comportamiento del sujeto se produce con posterioridad al delito de estafa informática, entendiendo así dichos autores la consumación del delito de estafa con el mero apoderamiento de las cuantías transferidas de la cuenta de la víctima. Sin embargo, otros autores estiman más apropiada la consideración de cooperación necesaria para el comportamiento de los muleros. Ello se entiende dado que el comportamiento de éstos no se produce por azar, dado que no solo se limitan a extraer y remitir a terceros países las sumas de capital (lo cual sí podría considerarse como una participación posterior al delito previo de estafa informática), sino que se produce una colaboración activa con el defraudador facilitando su cuenta bancaria en la que se recibirán las sumas estafadas y conociendo o debiendo conocer al realizar el

[160] FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 31.
[161] Cfr. OXMAN, N., *op.cit.* , pág. 216.

envío a terceros países siguiendo un razonamiento lógico el origen ilícito del mismo además de solicitar una contraprestación por ello[162].

Siguiendo la línea argumental del presente trabajo y en base a la tesis ya expuesta en apartados anteriores, se entiende la consumación del delito cuando se produce el perjuicio patrimonial en la víctima, lo cual coincidirá con el asiento contable y siendo el momento de consumación un elemento determinante para el apoyo de ambas teorías hemos de entender más acorde a dicha argumentación la segunda de las teorías expuestas por GOMEZ INIESTA. Existe, por parte del mulero, una participación al otorgar su cuenta al defraudador, y puesto que se produce la consumación una vez se produce la recepción por parte del mulero de la transferencia[163], parece lógico pensar que tal comportamiento del mulero, no puede considerarse postdelictual y, por ende, podemos apoyar su participación como cooperador necesario. Además, como apoyo a lo anterior puede destacarse la mención a la STS 533/2007, de 12 de junio, en la que una serie de sujetos que aceptaron la apertura de cuentas a su nombre en la entidad Citibank recibiendo transferencias no consentidas, por clientes de dicha entidad que fueron víctimas del *phishing*, y percibiendo por aquella colaboración una serie de comisiones, en concreto, expone la sentencia respecto a lo hechos descritos que *"se está ante un caso de delincuencia económica de tipo informático de naturaleza internacional en el que los recurrentes ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran, no quisieran saber –ignorancia deliberada–, o les fuera indiferente el origen del dinero que en cantidad tan relevante recibieron".*

Si bien pese a lo anterior, FERNANDEZ TERUELO expone, de una forma muy acertada, la necesidad de discernir entre el amplio abanico de posibilidades de actuación de estos "muleros", teniendo en cuenta que en determinadas ocasiones los mismos desconocen completamente su colaboración en actos ilícitos; así, imaginemos que el defraudador capta a los muleros mediando falsas ofertas laborales en las que para más inri se requerirá al sujeto la realización de algún tipo de tarea. Póngase, como ejemplo, la

[162] Cfr. GOMEZ INIESTA, D., *"Estafa y blanqueo de dinero a través de internet"*, *La Ley Penal*, número 105, 2013, págs. 33 y ss.
[163] FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 31.

realización de encuestas, haciendo creer que la comisión actúa como forma de pago por los servicios realizados. Supuesto más dudoso seria el relativo al posible conocimiento que pudiera llegar a tener el sujeto sobre el origen del capital, llegando a imaginar o suponer el origen ilícito de éste[164]. Se defenderá, para este caso, una postura similar a la expuesta en el párrafo anterior: una vez el mulero haya admitido la posibilidad de que su cuenta vaya a ser utilizada por el defraudador para transferir el capital de forma ilícita, se ha de entender concurrente el dolo eventual y por tanto ha de entenderse al sujeto como cooperador necesario de un delito de estafa informática.

6.2 Conexiones telefónicas fraudulentas

Se producen básicamente estas conexiones telefónicas fraudulentas a través de *dialers*[165]o *diallers,* que se definen por el Cambridge Dictionary como un software o programa que permite conectarse a un número de teléfono desde internet. Se produce así la instalación, en el dispositivo informático, de algún programa que realizara conexiones telefónicas a números de tarifación adicional sin el conocimiento del usuario en la gran mayoría de los casos, números de tarifación que por otro lado generaran un altísimo coste para el usuario. Dichos programas serán descargados normalmente mediante ficheros ejecutables (.exe) que son utilizados de forma nativa por Microsoft y Windows o bien mediante la descarga de controles Active X. Procede hablar de estafa informática cuando o bien se ha ocultado al usuario por completo la instalación de estos programas o cuando no se llega a ofrecer una visión nítida de las modificaciones que se realizaran en el dispositivo y de los gastos que conllevará la instalación de éste[166].

6.3 Fraude en las operaciones y transacciones en el comercio electrónico

Es notorio que en la actualidad el comercio electrónico ha sufrido un abismal auge, "obligando" a la mayoría de negocios a adaptarse a la nueva realidad social, la mayoría de hogares poseen internet, y la mayoría de los españoles portan teléfonos inteligentes o *smartphones* consigo que permiten una conexión a internet prácticamente desde cualquier

---

[164] *Ibidem*, pág. 33.

[165] http://dictionary.cambridge.org/es/diccionario/ingles/dialler?fallbackFrom=english-spanish&q=dialer (consulta 3 de enero de 2019).

[166] Cfr. FERNANDEZ TERUELO, J.G., *"Respuesta penal frente a fraudes cometidos en internet: Estafa, Estafa informática, y los nudos en la red", Revista de Derecho Penal y Criminología,* número 19, 2007, pág. 222.

lugar. Ya se habló al comienzo del presente trabajo de los sucesivos estudios realizados por el INE dentro del ámbito de la informática, haciendo especial énfasis en el ultimó publicado, en concreto del año 2017[167], en el cual puede apreciarse el gran auge que el comercio electrónico ha sufrido; así se expone que un 40 % de españoles realizó algún tipo de compra a través de internet. En relación a lo anterior, también puede aportarse un informe del CNMC relativo al tercer trimestre del año 2016 en el que se afirma que España ha alcanzado la cifra de facturación 6.166,8 millones de euros en términos de comercio electrónico[168].

No obstante, no está exento el comercio electrónico de conductas fraudulentas, atañen principalmente dichas conductas fraudulentas al pago del precio o a la efectiva entrega de la cosa, pudiendo así afectar tanto a consumidores como a empresarios[169].

6.4 Envió de correos electrónicos fraudulentos

Se trata en este apartado del uso de la técnica conocida como *spam* o envío de correos electrónicos masivos mediante los cuales se intentará hacer creer a la víctima que obtendrá un determinado beneficio, en la mayoría de los casos, se utiliza la excusa de un premio, una herencia, pagando una determinada cantidad de dinero motivando dicha inversión en la posterior recepción de cantidad superior a la "invertida". No debe confundirse este tipo de conducta fraudulenta con la de obtención de datos o claves dado que, en este caso, la conducta de la víctima se limita a entregar la cantidad solicitada por el defraudador normalmente como gastos de tramitación o como supuestos impuestos y no se le solicitan a este datos sensibles, así también puede también incluirse en tales correos números de teléfono ante posibles dudas en los que las victimas sufrirán un perjuicio patrimonial a causa de la alta tarifación entre otras posibilidades.

[167] http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70 (consulta 3 de enero de 2019).
[168] https://www.cnmc.es/2017-04-07-el-comercio-electronico-supera-en-espana-los-6100-millones-de-euros-en-el-tercer (consulta 26 de junio de 2017).
[169] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 33.

Sección 2ª: Las defraudaciones de fluido eléctrico y análogas

1. Concepto y denominación

Como se analizará *infra* en el apartado correspondiente a la evolución normativa y regulación actual de la presente sección, en el año 1944 se recogía ya por el Código Penal la figura de la defraudación de energía eléctrica en sus artículos 536 a 538, viéndose obligado posteriormente el legislador a una adaptación de la legislación en esta materia debido a los avances sociales y tecnológicos, ampliándose en este sentido la tipificación por el Código Penal de 1995 y sus sucesivas reformas.

Se recoge, así, por el artículo 255 del vigente Código Penal, la comisión de defraudaciones mediante mecanismos instalados para la defraudación, mediante la alteración maliciosa de las indicaciones o de los propios aparatos contadores o mediante cualquier otro medio clandestino que permita la utilización de energía eléctrica, gas, agua, telecomunicaciones, u otro elemento, energía o fluido ajeno. Y, por otro lado, se castiga por el artículo 256 del Código Penal, el uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular y causándole un perjuicio económico.

Son conductas caracterizadas por la comisión de una defraudación mediante el uso o utilización, bien de energía eléctrica, gas, agua, telecomunicaciones, u otro elemento, energía o fluido ajenos, bien de cualquier equipo terminal de telecomunicación, encontrándose ambas conductas ciertamente ligadas, pues, como se analizará en sucesivos apartados, en determinadas formulas específicas de comisión, como la defraudación de procesamiento, se produce no solo un "uso" ilícito de terminales (como por ejemplo ordenadores por su potencia de procesamiento de datos), sino también de energía eléctrica o redes de telecomunicación, pues estos equipos hacen uso de la misma, incrementándose el consumo eléctrico de forma exponencial a más potencia se requiere del equipo.

No debe por otra parte confundirse la figura del artículo 255 ya citada con la recogida por el artículo 283 del Código Penal, pues dispone este último que *"se impondrán las penas de prisión de seis meses a un año y multa de seis a dieciocho meses a los que, en perjuicio del consumidor, facturen cantidades superiores por productos o servicios cuyo costo o precio se mida por aparatos automáticos, mediante la alteración*

o manipulación de éstos", y si bien es manifiesta una cierta semejanza entre ambas figuras, se configura el delito del artículo 283 ya citado como un tipo protector de un bien jurídico supraindividual, el orden socioeconómico, y más concretamente, en la protección del interés de los consumidores en el abastecimiento de productos o servicios cuyo costo o precio se mide por medio de aparatos automáticos, entrando por ende en juego dicho precepto cuando son los propios suministradores de estos servicios (pues de otra manera no puede entenderse al tenor de la formula *"facturen"*) los que manipulan o alteran los aparatos automáticos encargados de indicar el consumo de los productos o servicios contratados y efectivamente utilizados por el consumidor; así, por ejemplo, dependerá la punición mediante un tipo u otro del sujeto que realice la alteración del contador, de realizarla el consumidor, se tipificará la conducta por el artículo 255 del Código Penal, y de realizarla el suministrador de los servicios o productos, se subsumirá la conducta en el artículo 283 del Código Penal.

2. Evolución normativa y regulación actual

Se recogía por el Decreto de 23 de diciembre de 1944, por el que se aprueba y promulga el Código Penal, texto refundido de 1944, según la autorización otorgada por la Ley de 19 de julio de 1944, en concreto, en su sección 4ª, capítulo IV, título XIII, libro II de dicho texto, los supuestos de defraudación de fluido eléctrico y análogas. Específicamente, en el artículo 536 que refería que *"será castigado con las penas de arresto mayor y multa del tanto al triplo del perjuicio causado el que cometiere defraudación utilizando ilícitamente energía eléctrica ajena por alguno de los medios siguientes: 1.º Instalando mecanismos para utilizarla. 2.º Valiéndose de dichos mecanismos para la misma utilización. 3º. Alterando maliciosamente las indicaciones o aparatos contadores"*; en su artículo 537, *"el que con ánimo de obtener lucro ilícito en perjuicio de consumidor, alterare maliciosamente las indicaciones o aparatos contadores de fluido eléctrico o cometiere cualquier otro género de defraudación, será castigado con multa de 1.000 a 5.000 pesetas, y caso de reincidencia, con arresto mayor y multa sobredicha"*; y por el artículo 538, que dispone: *"las penas señaladas en los dos artículos precedentes se aplicarán a las defraudaciones de gas, agua u otro elemento, energía o fluidos ajenos, cometidas por los medios en aquellos expresados".*

Posteriormente, en el año 1963, se modificó por el Decreto 691/1963, de 28 de marzo, por el que se aprueba el Texto revisado de 1963 del Código Penal, el artículo 536, al que se añade la formula *"sin que esta pueda ser inferior a 5.000 pesetas"* respecto de la pena de multa, manteniéndose el contenido en los mismos términos. Igualmente, se actualiza la cuantía recogida por el artículo 537, pasando la cuantía de 1.000 a 5.000 pesetas, a la cantidad de 5.000 a 50.000 pesetas.

Tras la aprobación de la Ley Orgánica 3/1989, de 21 de junio, de actualización del Código Penal, se incorporó la falta de defraudación de fluido eléctrico por el artículo 587.2º, disponiendo que *"los que cometieren estafa, apropiación indebida, o defraudación de electricidad, gas, agua, u otro elemento, energía o fluido, en cuantía no superior a 30.000 pesetas".*

Con el Código Penal de 1995, el artículo 255 recoge que *"será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes: 1.º Valiéndose de mecanismos instalados para realizar la defraudación. 2.º Alterando maliciosamente las indicaciones o aparatos contadores. 3.º Empleando cualesquiera otros medios clandestinos",* haciendo una modificación relevante del contenido, incluyendo o especificando ciertos modos de acción, realizando para ello una enumeración *numerus apertus,* y añadiendo expresamente una referencia a las telecomunicaciones como objeto material del delito. Por otro lado, se crea la figura recogida por el artículo 256 de dicho texto, la cual tipifica la utilización o uso ilícito de equipos o terminales de telecomunicación, disponiendo en concreto que *"el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses".* Pasa la falta relativa a estas conductas a recogerse por el artículo 623.4 del Código Penal, disponiendo en concreto que *"serán castigados con arresto de dos a seis fines de semana o multa de uno a dos meses: 4. Los que cometan estafa, apropiación indebida, o defraudación de electricidad, gas, agua u otro elemento, energía o fluido, o en equipos terminales de telecomunicación, en cuantía no superior a cincuenta mil pesetas",* sufriendo una modificación sustancial respecto de la redacción del año 1989.

Posteriormente, la modificación operada por la Ley Orgánica 15/2003, de 25 de noviembre, actualiza, debido al cambio de moneda, las cantidades de pesetas a euros, debiendo ser las defraudaciones superiores a 400 euros para el caso del artículo 255 del Código Penal, un perjuicio superior a 400 euros en el artículo 256 del Código Penal, y una cuantía no superior a 400 euros en el caso del artículo 623.4 del Código Penal; además, se modifica la falta del artículo 623.4 del Código Penal, disponiendo la misma que *"los que cometan estafa, apropiación indebida, o defraudación de electricidad, gas, agua u otro elemento, energía o fluido, o en equipos terminales de telecomunicación, en cuantía no superior a 400 euros".*

Tras la aprobación de la Ley Orgánica 1/2015, de 30 de marzo, se eliminan las faltas y se modifican ligeramente los artículos 255 y 256 del Código Penal, quedando la redacción del artículo 255 del Código Penal ahora dividida en 2 apartados, siendo el primero de ellos prácticamente similar al de la anterior redacción, pero sin requerirse para su apreciación de la concurrencia de un perjuicio con valor determinado, es decir, siendo típicas las conductas descritas con independencia del valor de la defraudación, pues deja de constituir el mismo un elemento del tipo. Al hilo de lo anterior, se incluye un apartado segundo (artículo 255.2 del Código Penal), que recoge un tipo atenuado por razón de la cuantía, y en concreto, dispone que *"si la cuantía de lo defraudado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses".* Por otro lado, se modifica el artículo 256 del Código Penal por la Ley Orgánica 1/2015, de 30 de marzo, dividiéndolo igualmente en 2 apartados, configurándose el artículo 256.2 del Código Penal como un tipo atenuado a razón de la cuantía, empleando el legislador la misma fórmula que para el artículo 255.2 del Código Penal: *"si la cuantía del perjuicio causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses"*. Finalmente, la redacción de estos dos preceptos queda como se expondrá a continuación, en el caso del artículo 255 del Código Penal: *"1. Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes: 1.º Valiéndose de mecanismos instalados para realizar la defraudación. 2.º Alterando maliciosamente las indicaciones o aparatos contadores. 3.º Empleando cualesquiera otros medios clandestinos. 2. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses",* y la del artículo 256: *"1. El que hiciere uso de cualquier equipo terminal de telecomunicación, sin*

consentimiento de su titular, y causando a éste un perjuicio económico, será castigado con la pena de multa de tres a doce meses. 2. Si la cuantía del perjuicio causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses".

3. Bien jurídico protegido

Se sitúan los preceptos relativos a estas conductas en la sección 3ª, del capítulo VI, relativo a las defraudaciones, del título XIII, correspondiente a los delitos contra el patrimonio y contra el orden socioeconómico, del libro II del Código Penal, lo cual implicaría, siguiendo como se hizo en los delitos de estafa informática, mediante la aplicación del criterio de la ubicación sistemática de los artículos 255 y 256 en el Código Penal, y en atención a la propia redacción del tipo, una protección del bien jurídico patrimonio en su vertiente individual, que se entiende lesionado por el uso no consentido y perjudicial, bien del suministro, bien de equipos terminales de comunicación.

4. Elementos de la punición

4.1 Ejecución

Se configuran los delitos recogidos por los artículos 255 y 256 del Código Penal como delitos de resultado, requiriendo ambos para su consumación como ocurría en los supuestos de estafa informática ya analizados, de la producción de un resultado, un perjuicio patrimonial, como consecuencia de la conducta y distinto de la misma[170], por ello, es posible la distinción de diversas fases en su ejecución, siendo posible la apreciación, tanto de la tentativa acabada como la inacabada recogidas por el artículo 16 del Código Penal[171]. Serán concurrentes, conforme a lo expuesto, la tentativa acabada, cuando se realicen el conjunto de actos ejecutivos necesarios para la consecución del resultado, pero éste, sin embargo, no llegue a producirse, es decir, cuando no se logre ocasionar perjuicio patrimonial al sujeto pasivo, y por otro lado, la tentativa inacabada, cuando se interrumpa involuntariamente la acción delictiva sin haber realizado el sujeto activo todos los actos ejecutivos necesarios para la producción del resultado; así, por ejemplo, no se requiere de un arduo ejercicio imaginativo para ejemplificar los supuestos

[170] LUZÓN PEÑA, D.M., *op.cit.*, pág. 165.
[171] REY HUIDOBRO, L.F, *op.cit.*, pág. 8.

de tentativa inacabada, siendo un claro caso el del sujeto que es encontrado *in fraganti* colocando los mecanismos o alterando las indicaciones sin llegar a realizar el conjunto de actos ejecutivos, por el contrario, respecto de la tentativa acabada, podría pensarse en aquellos supuestos en los que el sujeto tras la instalación de un mecanismo, no consigue la producción de la defraudación debido a un fallo del mismo o bien porque se corta la electricidad por motivos de mantenimiento y se encuentra el dispositivo antes de reanudar el servicio, no causando el mismo perjuicio alguno.

Respecto a la consumación de los tipos antedichos, puede extrapolarse la tesis de MESTRE DELGADO ya analizada en los delitos de estafa informática, pues el legislador ha construido de forma ciertamente similar dichas figuras: *"la consumación, que acaece cuando, a la ejecución completa de la acción típica, se produce el resultado prohibido por la norma, realizándose aquel concreto perjuicio patrimonial"*[172], produciéndose como ya se mencionó la consumación de los tipos de los artículos 255 y 256 del Código Penal una vez producido el resultado típico, es decir, el perjuicio patrimonial.

Si bien para este tipo de delitos no cabe duda de la posibilidad de comisión activa, es clara la inaplicabilidad de la figura de la omisión pura al no existir una previsión legal que tipifique la misma para este tipo de delitos (ello en virtud de lo dispuesto por el artículo 10 del Código Penal: *"son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley*"). Entraña sin embargo ciertas dudas la comisión por omisión de estas figuras, pues por las expresiones empleadas por el legislador, como por ejemplo en el artículo 255 del Código Penal (*"valiéndose de mecanismos instalados para realizar la defraudación*", *"alterando maliciosamente"* o *"empleando cualesquiera otros medios clandestinos")*, o en el artículo 256 del Código Penal (*"el que hiciere uso")*, hacen ver estas conductas como meramente activas; sin embargo, por previsión del artículo 11 del Código Penal, *"los delitos que consistan en la producción de un resultado sólo se entenderán cometidos por omisión cuando la no evitación del mismo, al infringir un especial deber jurídico del autor, equivalga, según el sentido del texto de la ley, a su causación. A tal efecto se equiparará la omisión a la acción: a) Cuando exista una específica obligación legal o contractual de actuar. b) Cuando el omitente haya creado una ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente"*, y siendo los delitos de los artículos 255 y 256 del Código Penal

[172] MESTRE DELGADO, E., *op.cit.*, pág. 408.

delitos de resultado, no se descartará la posibilidad de concurrencia de la figura de la comisión por omisión; sin embargo, se hace ciertamente difícil imaginar supuestos específicos donde se aprecie dicha figura.

Por otro lado, por previsión de lo dispuesto por el artículo 12 del Código Penal, en concreto, que *"las acciones u omisiones imprudentes sólo se castigarán cuando expresamente lo disponga la Ley",* al configurarse como delitos eminentemente dolosos, y dada la inexistencia de un precepto que tipifique la comisión imprudente, debe entenderse únicamente la posibilidad de comisión dolosa de este tipo de delitos.

Respecto de los actos preparatorios de provocación, conspiración y proposición, en los supuestos de los artículos 255 y 256 del Código Penal, a diferencia de los delitos de estafa informática, no es posible la punición de las mismas, puesto que, en virtud de lo expuesto por los artículos 17 y 18 del Código Penal, al no preverse por la ley su castigo respecto de estos tipos, y no siendo de aplicación a estos supuestos lo dispuesto por el artículo 269 del Código Penal como sí ocurría en los supuestos de estafa informática, no puede entenderse su punición.

4.2 Autoría y participación

Son de perfecta aplicación a los tipos de los artículos 255 y 256 del Código Penal, los artículos 28 y 29 del mismo texto, relativos a la autoría y participación. Y, si bien para el caso de los artículos 255 y 256 del Código Penal, no prevé el legislador expresamente, como así hizo en otras figuras, como el artículo 248.2.b) del Código Penal, conductas como la fabricación, introducción posesión o facilitación de medios para la realización de estas defraudaciones, podrán reconducirse a la figura de la cooperación necesaria del artículo 28 del Código Penal, las conductas relativas a la instalación o puesta a disposición a otro sujeto a sabiendas de su fin, de medios específicos para la realización de las defraudaciones ya citadas. En este sentido, FARALDO CABANA refiere que *"por su parte, quien instala o proporciona los mecanismos o medios en cuestión, a sabiendas de que serán utilizados para cometer la defraudación, responde como cooperador necesario del delito cometido por el consumidor o usuario que se beneficia de su uso"*[173]. Igualmente, no se prevé por el legislador para los supuestos del artículo 255 y 256 del

[173] FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación"* en *Un derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz*, Tirant lo Blanch, Valencia, 2011, págs. 363 y ss.

Código Penal, responsabilidad penal de persona jurídica, debiendo recordase que, por previsión del artículo 31 bis del Código Penal, solo serán jurídicamente responsables las mismas *"en los supuestos previstos en este Código",* no existiendo respecto de los citados tipos referencia alguna.

4.3 Circunstancias

Son aplicables para los tipos de los artículos 255 y 256 del Código Penal casi todas las circunstancias atenuantes y agravantes recogidas en el Código Penal; en este sentido, dada la propia redacción del artículo 22.1º del Código Penal, cuando expone que *"hay alevosía cuando el culpable comete cualquiera de los delitos contra las personas"*, debe entenderse la inaplicabilidad de dicha circunstancia agravante, por otro lado, pese a que no se desprende de forma literal del propio precepto como en el caso anterior, puede entenderse igualmente inaplicable la agravación del artículo 20.5º del Código Penal relativa al ensañamiento, dado que difícilmente se podrá, en unos delitos de carácter patrimonial, aumentar deliberada e inhumanamente el sufrimiento de la víctima. Por otro lado, la circunstancia mixta de parentesco prevista por el artículo 23 del Código Penal, será de aplicación en virtud de lo dispuesto por el artículo 268 del Código Penal como eximente de responsabilidad criminal, ello siempre y cuando no concurran violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad.

4.4 Penalidad

Puede observarse en primer lugar, respecto de las figuras recogidas por los artículos 255 y 256, la modalidad leve de ambos delitos, pues al mantener una construcción similar, el legislador ha empleado en ambas figuras la siguiente formula: *"si la cuantía de lo defraudado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses"*, estableciéndose, así, en los artículos 255.2 y 256.2 del Código Penal, una barrera estructuralmente similar a la recogida por los delitos de estafa, y más concretamente, por el párrafo segundo del artículo 249 del Código Penal, estableciéndose una pena multa de uno a tres meses (inferior a la de los artículos 255 y 256 del Código Penal) para defraudaciones que no excedan los 400 euros, por otro lado, de superar tal

barrera o limite económico, se impondrá en atención a los artículos 255.1 y 256.1 del Código Penal la pena de tres a doce meses de multa.

En atención a la redacción del artículo 31 del Código Penal, y dada la ausencia de previsión para los delitos de los artículos 255 y 256 del Código Penal, como ya se puntualizó, no es posible la apreciación de responsabilidad penal de personas jurídicas.

Como ha podido observarse a lo largo de la presente sección, no son pocas las similitudes entre las figuras de los artículos 255 y 256 del Código Penal con las estafas, siendo quizá ello el motivo por el que el legislador engloba estos delitos bajo el capítulo VI, relativo a las defraudaciones, dentro del título XIII, del libro II del Código Penal. Así, como ocurría con las estafas (en el caso de las estafas informáticas debido al automatismo inherente a dichas conductas), los autores de las defraudaciones tienden a emplear de forma frecuente las mismas dinámicas comisivas, repitiendo estas infracciones de forma continuada contra un mismo patrimonio o contra una pluralidad de ellos, es por ello, que es perfectamente viable la aplicación de lo dispuesto por el artículo 74 del Código Penal, en lo relativo a la continuidad delictiva, debiendo hacer especial hincapié, puesto que estas conductas atentan contra el patrimonio, en la formula expuesta por el artículo 74.2 del Código Penal, imponiéndose la pena en atención al perjuicio total causado, estableciendo el juez o tribunal la pena superior en uno o dos grados en la extensión conveniente si el hecho revistiere notoria gravedad o hubiere perjudicado a una generalidad de personas[174]. Continuidad que, en los delitos relacionados con los sistemas informáticos o de telecomunicaciones, goza de mayor relevancia, pues se caracterizan aquellas conductas por gozar de un cierto dinamismo, debido al automatismo inherente al de los medios empleados que permiten generalmente, mediante una única instrucción, comando u orden del sujeto activo, la repetición de la conducta.

Por otro lado, si bien existe una estrecha relación entre las conductas recogidas por el artículo 255 y 256 del Código Penal, pues normalmente el perjuicio producido por el uso o la utilización de equipos de telecomunicaciones no es otro que el de los servicios empleados por dichos equipos (como la energía eléctrica, tarifas de servicios de telecomunicación, entre otras), no puede hablarse en estos casos de concurso de delitos entre ambas figuras, puesto que ello sería contrario al principio *non bis in ídem*, hablándose así, respecto de estos casos, de la concurrencia de un concurso de leyes

[174] MESTRE DELGADO, E., *op.cit.*, pág. 408 y 409.

recogido por el artículo 8 del Código Penal. Se debe así acudir a lo dispuesto por el artículo 8.1ª del Código Penal, dado que, el tipo de uso o utilización de equipos terminales de telecomunicación del artículo 256 del Código Penal, *per se*, parece gozar de una cierta especialidad frente al delito de defraudación de energía y análogas (si bien no parece apreciarse de forma tan clara como ocurre en los supuestos de homicidio del artículo 138 del Código Penal y de eutanasia del artículo 143 del mismo texto, donde el último de ellos ha de aplicarse con preferencia al de la figura genérica bajo ciertas circunstancias[175]), aún de producirse el perjuicio debido al empleo por el equipo terminal de telecomunicación, bien de energía eléctrica, bien de redes de telecomunicación (como son las redes Wi-Fi, planes de datos móviles, redes de telefonía, entre otras), lo que caracteriza la conducta es la efectiva utilización no consentida de un equipo terminal de telecomunicación ajeno sin el que en principio, no existiría dicho perjuicio derivado del uso por el mismo de redes de suministro, así, por ejemplo, el sujeto que mediante un uso no autorizado de un equipo terminal de telecomunicación, como pudiere ser un *smartphone* o teléfono inteligente ajeno, que hace uso del mismo para la realización de llamadas internacionales (de gran coste para el titular del mismo) o hace uso de la tarifa de datos móviles, habrá de ser encuadrado en el artículo 256 del Código Penal, puesto que si bien se emplea por el dispositivo la red de telefonía para la realización de las llamadas (las cuales ocasionarán un aumento del coste del suministro telefónico contratado), lo que en un principio caracterizaría la conducta, es el uso no consentido del equipo, que deviene en un posterior perjuicio patrimonial para el titular del terminal. Sin embargo, dicha discusión adquiere únicamente relevancia en un plano teórico, pues el marco punitivo de ambas conductas es idéntico.

Respecto de la posibilidad de apreciación conjunta a otras figuras, es decir, en concurso de delitos, no parece en principio existir inconveniente para ello, no obstante, es necesaria la realización de una serie de puntualizaciones.

Así, por ejemplo, respecto de la conducta recogida por el artículo 247 del Código Penal, relativa a la distracción del curso de las aguas (recalcando la expresión *"la utilidad reportada"* recogida por el artículo 247.2 del Código Penal), y de la amplia redacción del artículo 255 del Código Penal, cabe puntualizar que en principio, si bien podrían

[175] Cfr. JEAN PIERRE MATUS, A., *"Los criterios de distinción entre el concurso de leyes y las restantes figuras concursales en el código penal español de 1995", Anuario de derecho penal y ciencias penales*, tomo 58, 2005, *pág. 470.*

confundirse ambas figuras tras una primera lectura, parecen ser aplicables a supuestos inminentemente distintos, pues el primero de ellos habrá de interpretarse en conjunto con el Real Decreto Legislativo 1/2001, de 20 de julio, por el que se aprueba el texto refundido de la Ley de Aguas; así, como bien señala la SAP Alicante 565/2014, de 31 de octubre, relativa a una persona que con ánimo de obtener un ilícito lucro, procedió, directamente o a través de terceras personas pero con su conocimiento y consentimiento, a colocar una manguera en la salida de agua de la vivienda colindante, para a continuación extraer agua durante varios días llenando así su piscina y realizando operaciones de limpieza a presión, causando un perjuicio de 1.125,26 euros, *"el hecho enjuiciado no es constitutivo de un delito de artículo 247. Dicho precepto contempla un supuesto muy específico que se conecta con el artículo 2 de la Ley de Aguas cuyo Texto Refundido fue aprobado por Real Decreto Legislativo 1/01, de 20 de julio […]. El tipo se refiere a la distracción de «aguas de uso público o privativo de su curso...» por «curso» debe entenderse el movimiento del agua que se traslada por un cauce, como pueden ser los ríos, arroyos o incluso las acequias para riego (artículo 2 b de la LA). El agua que discurre por dichos espacios es un bien público como establece el artículo 1 de la Ley de Aguas, pero su uso puede ser público o privativo en los supuestos qué dicha norma contempla, de ahí la dicción del artículo 247 CP. Por tanto, nunca el agua que discurre por tuberías de uso doméstico puede ser incluida en el ámbito del tipo y sí, al contrario, del de las defraudaciones del artículo 255 CP"*, siendo el objeto de protección de ambos tipos distinto, por un lado, en el artículo 247 del Código Penal, el agua de uso público o privativo en su curso normal o en embalse natural o artificial, y por otro lado, el artículo 255 del mismo texto que requiere de agua sujeta a suministro, cuyo consumo sea posible contabilizar mediante mecanismos creados a tal efecto. En este sentido, MESTRE DELGADO dice: *"creo que el concurso es sólo aparente, y que cada uno de los preceptos en principio concurrentes tiene de sus propios y específicos ámbitos de aplicación, no coincidentes: el tipo de usurpación se aplica tan sólo cuando el sujeto activo asume facultades de dominio y disposición, que no le corresponden, sobre el curso del agua, que distrae para obtener (para sí o para un tercero) un beneficio (por ejemplo: un agricultor que decide desviar el curso para que la cercanía de las aguas permita un incremento de regadío en las tierras de su propiedad); en tanto el delito de defraudación concurre cuando el autor del hecho desvía el curso de las aguas como medio para cargar a un tercero determinados constes que en otro caso el debería asumir (por ejemplo, el agricultor que altera el curso para que las aguas no pasen por su contado de consumo, sino por el del propietario del*

fundo vecino, y después de ese tramo vuelvan a su flujo habitual)"[176]. En todo caso, de no entender lo anterior, podría plantearse la posibilidad de existencia de un concurso de leyes entre ambas figuras, resolviéndose el mismo por aplicación del artículo 8 del Código Penal, pero no parece por lo expuesto viable la posibilidad de concurrencia de un concurso de delitos.

Por otro lado, respecto de la utilización o uso no consentido de equipos terminales de telecomunicación ajenos para la realización de una transferencia de cualquier activo patrimonial igualmente no consentida, en relación al artículo 248.2 del Código Penal, habrá de entenderse, como bien expone MESTRE DELGADO, la infracción de *"dos preceptos concurrentes, y ninguno de ellos absorbe por completo el desvalor de la acción conjunta, por lo que no resultan aplicables las normas del concurso de leyes, sino las del concurso de delitos, y más específicamente las del concurso medial"*[177], pues, como señala FARALDO CABANA, al referenciar la Consulta 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago, *"no se puede decir lo mismo de la concurrencia del concepto «transferencia de activo patrimonial», ya que [...] no se transfiere propiamente ningún bien del patrimonio de un sujeto al de otro, sino que simplemente se disfruta de un servicio de manera inmediata"*, llegando la citada autora a la conclusión de que *"la manipulación informática o el artificio semejante empleado en el ámbito de los servicios de telecomunicaciones […] para conseguir el servicio sin pagar la contraprestación, no responden, en efecto, a la estructura de la estafa informática, delito en el cual la transferencia de activos patrimoniales es el resultado intermedio que debe llevar a la causación de un perjuicio patrimonial a la víctima"*[178], no pudiendo en síntesis de lo anterior hablar en el presente caso de concurso de leyes, siendo viable la apreciación de un concurso de delitos.

Finalmente, otra cuestión sería la de entender concurrente el tipo de daños informáticos (que se analizará en posteriores secciones), pues, como se ejemplificará en el apartado correspondiente a las defraudaciones de procesamiento computacional (artículo 256 del Código Penal), en conductas como el *cryptojacking*, donde se produce una mayor exigencia o aumento del trabajo de procesamiento del sistema, es posible, en

[176] MESTRE DELGADO, E., *op.cit.*, pág. 409.
[177] *Ibidem*, pág. 410.
[178] FARALDO CABANA, P., "*Defraudación de telecomunicaciones y uso…"*, págs. 363 y ss.

los casos más extremos, una obstaculización o interrupción del sistema informático debido al alto nivel de procesamiento al que se expone el mismo, y no siendo extraña para su realización una alteración de datos informáticos o programas para controlar de forma remota el sistema, entendiendo por ende para estos casos, al igual que ocurría con los supuestos de estafa informática *supra* mencionado, y como bien señala MESTRE DELGADO, se produce en estos casos la infracción de *"dos preceptos concurrentes, y ninguno de ellos absorbe por completo el desvalor de la acción conjunta, por lo que no resultan aplicables las normas del concurso de leyes, sino las del concurso de delitos, y más específicamente las del concurso medial"*[179]. Y si bien podría defenderse que, en principio, el sujeto que instala malware para el minado no busca (es decir, no existe en principio en él un *"ánimus damnandi"* o *"ánimus nocendi"*) la interrupción u obstaculización del sistema, o el borrado o alteración de datos, podría ante esa alegación reconducirse tal cuestión al dolo eventual, pues el sujeto, pese a no pretender dicho resultado podría representarse la posibilidad del mismo, o inclusive el dolo "indirecto" o de segundo grado también llamado dolo de consecuencias necesarias, puesto que, dados los conocimientos mínimos necesarios de informática necesarios para la realización de la conducta, el sujeto sea conocedor de la necesidad de dañar o alterar el sistema para la realización de la defraudación, como bien señala LUZÓN PEÑA respecto de este tipo de dolo, *"la intención o propósito que persigue el sujeto no es precisamente la realización del tipo, sino la consecución de otro objetivo, pero sabe que a tal acción encaminada a otro fin va unida necesariamente y con seguridad la realización de todos los elementos de un tipo delictivo[...] cuya producción por tanto, aunque no le guste, también acepta"*[180].

4.5 Responsabilidad civil

Será de aplicación lo dispuesto en el título V, del libro I, del Código Penal; sin embargo, pueden destacarse los artículos 109.1 del Código Penal en cuanto refiere que *"la ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados"*, y también el artículo 110 del Código Penal relativo a la extensión de la responsabilidad civil. No debe olvidarse tampoco por su relevancia el artículo 116 del Código Penal cuando expone que

[179] MESTRE DELGADO, E., *op.cit*., pág. 410.
[180] LUZÓN PEÑA, D.M., *op.cit.*, pág. 244.

"toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que deba responder cada uno", y también que *"los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables".*

5 Elementos del tipo

5.1 Defraudaciones de energía y análogas

La acción típica del tipo del artículo 255 del Código Penal la configura el uso o utilización, configurándose los medios de acción de forma alternativa, pudiendo realizarse la misma mediante mecanismos instalados para la defraudación, mediante la alteración maliciosa de las indicaciones o de los propios aparatos contadores, o mediante cualquier otro medio clandestino, una clausula empleada por el legislador que otorga al tipo una apertura conceptual que como en otros delitos ya analizados, parece confrontar con los principios de legalidad y seguridad jurídica, y con la que el legislador parece querer evitar supuestos de laguna legal debido al rápido avance de la tecnología y de los distintos medios defraudatorios. Respecto del objeto material del delito, lo conforman la energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajeno, empleando igualmente una formula ciertamente abierta, pues con la expresión *"u otro elemento, energía o fluido ajeno",* se permite el encuadre de cualquier tipo de objeto material semejante que pudiere surgir en un futuro; así, como bien señala MANZANARES SAMANIEGO, *"se trata de energías o fluidos que son objeto de un suministro en cuyo curso se produce la defraudación. En el caso de que la energía o el fluido fueran el contenido de un recipiente (bombona de butano, batería, bidón de agua, etc.), no se aplicará el artículo 255, sino el tipo correspondiente de hurto, robo o apropiación indebida"*[181], y en la misma línea, GONZALEZ RUS, cuando refiere que *"la mención a los «fluidos» puede acoger tanto a líquidos o gases (gasolina, gas ciudad, que se suministra por redes), como a cualquiera elementos capaces de traducirse en*

[181] MANZANARES SAMANIEGO, J.L., *Comentarios al Código Penal. Tras las leyes orgánicas 1/2015, de 30 de marzo, y 2/2015, de 30 de marzo*, Editorial La Ley, Madrid, 2016, en recurso electrónico La Ley 3219/2016.

fenómenos físicos de naturaleza magnética, calórica, luminosa, etc., económicamente cuantificables; por ejemplo la energía solar. Las telecomunicaciones a las que se alude incluyen al teléfono, televisión por cable, transmisión de datos, recepciones de ondas"[182]. Finalmente, consiste el resultado típico en la defraudación del tercero que se materializa inevitablemente en un concreto perjuicio patrimonial[183].

5.2 Uso no autorizado de terminales de comunicación

Se configura la acción típica del artículo 256 del Código Penal como el uso o utilización no autorizada o abusiva del objeto material del delito, conformándose dicho objeto, por cualquier equipo terminal de telecomunicación (entiendo la RAE por equipo, el *"conjunto de aparatos constituido por una computadora y sus periféricos";* por computadora el *"que computa (calcula)";* o de forma más específica, referido a la computadora electrónica, aquella *"maquina electrónica que, mediante determinados programas, permite almacenar y tratar información, y resolver problemas de diversa índole";* y por telecomunicación, un *"sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos"*), describiéndose de forma muy correcta por MANZANARES SAMANIEGO, cuando refiere que, *"por equipo terminal de telecomunicación se entiende los puntos extremos de un medio de comunicación a distancia, al margen de que se utilicen impulsos eléctricos o electrónicos, ondas hertzianas u otras energías susceptibles de transmitir imágenes, signos o palabras, como es el caso del teléfono, el fax, el correo electrónico o las comunicaciones inalámbricas"*, no pudiendo entender subsumible por ende en el artículo 256 del Código Penal, en atención a lo expuesto, y como correctamente refiere FARALDO CABANA[184], la utilización de tarjetas SIM y análogas, o de claves de acceso a determinados servicios, colocadas o introducidas en terminales propios pues no son encuadrables en la descripción de *"equipo terminal de telecomunicación"* del citado artículo, y en concreto defiende la citad autora que *"la vigencia del principio de legalidad y la autonomía del Derecho penal obligan, en mi opinión, a optar por un concepto restrictivo de equipo de telecomunicaciones, más próximo a la definición de equipo terminal ofrecida por la Ley*

[182] GONZALEZ RUS, J.J., *"Delitos contra el patrimonio y contra el orden socioeconómico (VI Apropiación Indebida. Defraudaciones de Fluido Eléctrico y análogas"*, en *Derecho Penal Español: Parte Especial*, Dykinson, Madrid, 2005, pág. 541.
[183] MESTRE DELGADO, E., *op.cit.*, pág. 405.
[184] FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso…"*, págs. 363 y ss.

General de Telecomunicaciones. Así pues, en relación a este concepto debe entenderse que «cuando el tipo penal consigna equipo terminal de telecomunicaciones, sólo puede referirse a aquel equipo que por sí solo, y sin ningún aditamento, puede realizar y recibir comunicaciones, es decir a un equipo completo que constará, en caso de teléfonos móviles, tanto del equipo físico, como del programa que se halla incorporado normalmente a una tarjeta»"[185]*;* así, por ejemplo, el sujeto que meramente emplea una tarjeta SIM, una tarjeta de televisión, o introduce una clave ajena sin consentimiento de su titular para el disfrute de ciertos servicios y la emplea en su propio dispositivo, incurriría en un delito del artículo 255.3º del Código Penal, cuestión que sería diferente de emplearse el teléfono, decodificador o equipo ajeno de forma no consentida, en cuyo caso si podría hablarse de un delito del artículo 256 del Código Penal.

Respecto del resultado previsto por el tipo, en concreto, y a diferencia del caso expuesto por el artículo 255, donde se entiende implícito, se exige de forma expresa la necesidad de concurrencia de un perjuicio económico al titular del equipo de telecomunicaciones. Por otro lado, conviene no olvidar la incorporación del consentimiento como elemento del tipo positivo, mediante la formulada *"sin consentimiento de su titular"*, debiendo por ende producirse un uso no consentido de equipos de telecomunicación, funcionando el consentimiento del titular de dichos equipos como una causa de exclusión de la tipicidad o de atipicidad, excluyéndose la relevancia penal para aquellos casos en los que existiere consentimiento expreso o tácito (teniendo este mayores dificultades a la hora de su prueba)[186].

6. Formulas específicas

Si bien podrían exponerse en el presente epígrafe un número elevado de fórmulas específicas de comisión, pues los tipos de los artículos 255 y 256 del Código Penal, emplean como ya se analizó *supra* formulas abiertas que permiten la subsunción de conductas ciertamente dispares, se expondrán a continuación solamente algunas de ellas, pues se busca realizar una mera ejemplificación de ciertas formas específicas para un mejor estudio y asimilación del contenido de la presente sección.

[185] FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso…"*, págs. 363 y ss.
[186] Cfr. MESTRE DELGADO, E., *op.cit.*, pág. 407.

6.1 Formulas específicas de defraudación de energía y telecomunicaciones

Siguiendo la propia redacción del tipo del artículo 255 del Código Penal, un claro ejemplo de formula especifica de ejecución son las conductas de prevalimiento de mecanismos instalados para la realización de las defraudaciones, donde pueden encuadrarse clásicas fórmulas de realización de la conducta, como son, desvíos de fluidos hídricos, modificaciones o instalaciones en contadores de energía eléctrica ("enganches" o conexiones indebidas, puentes en el cableado, entre otras). Igualmente, se tipifica expresamente por el propio tipo la alteración maliciosa de indicaciones o aparatos contadores, pues consiste la misma en una de las principales formulas específicas de defraudación del suministro, como por ejemplo el sujeto que dispone de las llaves de los contadores de su vivienda y hace un puente para cargarle el consumo a un vecino o altera los datos de dicho contador para pagar una cantidad inferior a la consumida. Por otro lado, bajo la redacción excesivamente amplia del artículo 255.1.3º del Código Penal, cabe el encuadre de prácticamente cualquier conducta tendente a estas defraudaciones, destacable el caso de las defraudaciones de las señales de telecomunicación, en concreto, el de las señales de televisión por satélite, o por cable, conducta que se realiza mediante la utilización de aparatos o receptores de señal que permiten la visualización del contenido sin pagar la correspondiente tarifa; ello puede observarse por ejemplo en las SSAP de Ávila 186/2010, de 30 de noviembre, y de Illes Balears 16/2006, de 18 de enero (en la que se emplea una tarjeta decodificadora no autorizada, fabricada para acceder a canales de televisión sin abonar la correspondiente tarifa). Como ya se mencionó, se entiende en este trabajo que el empleo de materiales no encuadrables en la definición de equipo informático realizada por el artículo 256 del Código Penal, como, por ejemplo, el uso de tarjetas SIM, tarjetas de televisión, códigos de acceso o contraseñas, empleadas en dispositivos propios, tendría encaje en el artículo 255.3º del Código Penal.

6.2 Defraudación de procesamiento computacional

Defraudación encuadrable dentro del tipo del artículo 256 del Código Penal, que si bien es expuesto por autores como ROVIRA DEL CANTO bajo la denominación de hurto de tiempo informático, merece una denominación distinta, como sería por ejemplo la de "defraudación de procesamiento computacional"; sin embargo, como bien refiere el

citado autor, consiste la misma en *"la utilización no autorizada del tiempo de procesamiento informático"*[187], pudiendo darse de una forma más clásica, como por ejemplo, accediendo de forma física al equipo con el consiguiente perjuicio ocasionado al titular de los mismos, o bien, mediante métodos más sofisticados y actuales, como el *cryptojacking.*

Consiste el *cryptojacking* en la utilización o uso no autorizado de sistemas informáticos (como tabletas, teléfonos inteligentes, ordenadores, entre otros) para el minado de criptomonedas como Bitcoin o Ethereum, entre otras. Ello se consigue de forma habitual mediante el envío de correos electrónicos maliciosos cargados de malware camuflado como documentos, entre otros medios, mediante los que se consigue instalar códigos que permiten el minado de criptomonedas (es decir, la utilización de la potencia del procesamiento de datos del dispositivo del usuario, para la resolución de operaciones complejas por las que se recibirá en compensación un determinado porcentaje de moneda virtual que goza de un valor de mercado similar al de las acciones cotizadas en bolsa, dependiendo el mismo de la oferta y demanda de tal moneda) con el consiguiente perjuicio ocasionado al usuario o titular del equipo o sistema, que sufre no solo una ralentización o disminución del rendimiento del mismo, sino que además, puede ver incrementada la facturación de la electricidad debido a la sobrecarga de procesamiento generada en el sistema, pudiendo llegar incluso en el peor de los casos a provocar tal sobrecarga de trabajo un desgaste prematuro de componentes del sistema debido al calor producido en el equipo[188]. No se requiere así de excesivo esfuerzo para la realización de estas conductas, existiendo modalidades más perfeccionadas en las que ni siquiera se requiere de una instalación de malware en el dispositivo; así, pueden apreciarse en los supuestos en los que se emplean los conocidos como *web browser miner*, donde se hace uso de *scripts* en páginas web, produciéndose el secuestro de velocidad de procesamiento cuando la víctima accede al sitio web infectado o cuando aparecen *banners* o publicidad en los que los *script* se ejecutan de forma automática[189].

Se configura como una conducta que, si bien parece tener poca entidad a nivel de defraudación de un único usuario, adquiere mayor relevancia cuando se ataca, bien a

[187] ROVIRA DEL CANTO, E., *op.cit.*, pág. 205.
[188] Cfr. https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html (consulta 4 de enero de 2019).
[189] Cfr. https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html (consulta 4 de enero de 2019).

empresas especializadas en el minado de criptomonedas, las cuales pueden denominarse como "minas", o bien, mediante el ataque realizado en masa a un número indeterminado de equipos.

6.3 Otras fórmulas

Como recoge el artículo 256 del Código Penal, se exige únicamente un uso no consentido de cualquier equipo terminal de telecomunicaciones que cause un perjuicio económico a su titular; así por ejemplo puede mencionarse la SAP Valladolid 394/2014, de 22 de septiembre, en la que un sujeto, haciendo uso del equipo terminal de telecomunicaciones empleado para el sistema de averías del ascensor de una Comunidad de Propietarios, que servía para realizar las llamadas de emergencia, sin consentimiento de la Comunidad de Propietarios, se benefició del mismo para su uso particular, generando gastos superiores a los cuatrocientos euros, siendo esta resolución un ejemplo claro de fórmulas las clásicas o menos refinadas e realización de la conducta, siendo igualmente imaginables diversos supuestos, como por ejemplo, el de un trabajador/a doméstico que realiza llamadas internacionales que no se encuentran incluidas en el plan telefónico contratado por el titular de la línea o del agotamiento de la tarifa contratada por el titular de un contrato de datos móviles realizando tareas ajenas a las propias de sus competencias laborales con el equipo, llegando en casos extremos a abonar el titular del contrato al abono de paquetes de datos debido al agotamiento de su tarifa contratada, entre otras.

Igualmente remarcables, por su mayor perfeccionamiento, son los supuestos expuestos por FARALDO CABANA[190] cuando refiere la existencia de conductas como el *phreaking* (formas de *hacking* orientadas a la telefonía y estrechamente vinculadas con la electrónica, centrada especialmente en la realización de llamadas gratuitas mediante diversas técnicas) o el *piggybacking* (que no es otra cosa que la conexión no consentida a redes WI-FI).

[190] FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso…",* págs. 363 y ss.

Sección 3ª: El daño informático

1. Concepto y denominación

1.1 El tipo tradicional de daños

Queda tipificado el tipo básico o tradicional de daños por el artículo 263.1 del Código Penal, pudiendo definirse los delitos tradicionales de daños, dada la configuración residual o negativa de los mismos operada por el legislador, como aquellos actos que atentan contra la propiedad (susceptible de valoración económica), causando deterioros, menoscabos o la propia destrucción de la misma independientemente del perjuicio patrimonial que el daño pueda ocasionar[191], es decir, sin perjuicio de las responsabilidades civiles que a causa de los menoscabos generados por tal causa, puedan reclamar los poseedores legítimos del bien dañado[192], funcionando el perjuicio patrimonial como un mero factor determinante de la responsabilidad civil.

Son delitos que si bien para su concurrencia no requieren de la apreciación o concurrencia de ánimo de lucro o de enriquecimiento del sujeto pasivo, requieren sin embargo, de un cierto *"ánimus damnandi"* o *"ánimus nocendi",* es decir, de un ánimo de dañar, que puede o no tener un móvil especifico (que de existir, sería del todo irrelevante pues no se exige su concurrencia para la apreciación del daño en términos penales)[193].

Se configura además, por su propia naturaleza, como un delito común de resultado, es decir, que es posible discernir, primero, una acción típica, consistente en atención al propio tipo en un indeterminado número de conductas en tanto se realiza una determinación indirecta de la acción dado el carácter residual construido por el legislador, segundo, el objeto material del delito, configurándose como tal la propiedad ajena y, tercero, un resultado, consistente en la causación de un daño sobre el citado objeto de protección. Y que, por otro lado, pueden ser realizados por cualquier sujeto, sin necesidad de concurrencia de ninguna circunstancia o condición especial[194], salvo eso sí, los daños

[191] MUÑOZ CONDE, F., *Derecho penal. Parte espe…,* pág. 415.
[192] MESTRE DELGADO, E., *op.cit.*, pág. 410.
[193] Cfr. GARCIA VALDES, C., MESTRE DELGADO, E., FIGUEROA NAVARRO, C., *op.cit.*, pág. 149.
[194] MESTRE DELGADO, E., *op.cit.*, pág. 411.

contra cosa propia recogidos por el artículo 289 del Código Penal, en los que sí se requerirá de la condición de propietario de la cosa objeto del daño, cuando la misma mantuviere una utilidad social, cultural o se encontraré bajo deberes legales impuestos en interés de la comunidad.

Se prevé por el legislador un tipo privilegiado en cuanto el artículo 263.1 establece en su segundo párrafo que, *"si la cuantía del daño causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses".*

Igualmente, existen, en atención a lo dispuesto por el artículo 263.2 del Código Penal, una serie de subtipos agravados en atención a determinadas circunstancias, recogidas por el propio tipo: *"será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el apartado anterior, si concurriere alguno de los supuestos siguientes: 1.º Que se realicen para impedir el libre ejercicio de la autoridad o como consecuencia de acciones ejecutadas en el ejercicio de sus funciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales. 2.º Que se cause por cualquier medio, infección o contagio de ganado. 3.º Que se empleen sustancias venenosas o corrosivas. 4.º Que afecten a bienes de dominio o uso público o comunal. 5.º Que arruinen al perjudicado o se le coloque en grave situación económica. 6.º Se hayan ocasionado daños de especial gravedad o afectado a los intereses generales".*

Se recogen también las figuras cualificadas relativas a los delitos de daños informáticos recogidas en los artículos 264, 264 bis, 264 ter y 264 quater del Código Penal, que se analizaran *infra* para evitar la redundancia que supondría su exposición en el presente apartado.

Se recogen además por los artículos 265 y 266 del Código Penal, otra serie de tipos cualificados agravados, relativos al daño en los términos anteriormente expuestos de *"obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad"* para el caso del artículo 265 del Código Penal, o de la comisión de daños mediante incendio, la provocación de

explosiones, el uso de medios similares de potencia destructiva, que generen bien un riesgo de explosión de cierta relevancia o daños de especial gravedad poniendo en peligro la vida o la integridad de las personas para el caso del artículo 266 del Código Penal.

Existe un manifiesto desorden en cuanto a la sistemática seguida por el legislador respecto a los delitos de daños puesto que los distintos preceptos se encuentran diseminados a lo largo del Código Penal; así, por ejemplo, se recogen por el artículo 323 del Código Penal las conductas relativas al daño de bienes de valor artístico, histórico, científico, cultural monumental o en yacimientos arqueológicos, por el artículo 324 del Código Penal los daños en archivos, registros, museos, bibliotecas, centros docentes, gabinetes científicos o instituciones análogas o en bienes de valor artístico, cultural, histórico, científico, monumental o en yacimientos arqueológicos de cuantía superior a 400 euros y cometidos por imprudencia, por el artículo 351 del Código Penal los delitos de incendio que no supongan un peligro para la vida o la integridad física de las personas y por el artículo 560 los daños a líneas de telecomunicaciones, correspondencia postal, líneas férreas o conducciones o transmisiones de agua, gas o electricidad.

Respecto a los delitos de daños, cabe la posibilidad de apreciación no solo de comisión dolosa sino también imprudente, en atención a los artículos 12 y 267 del Código Penal, en tanto este último recoge que *"los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos"*, previéndose además en el artículo la necesidad de persecución previa denuncia de la persona agraviada o de su representante legal y reconociendo en su párrafo tercero, la posibilidad de perdón del ofendido o de su representante legal, por el cual se extinguirá la acción penal, sin perjuicio de la posibilidad de reclamación, por vía civil, de la cuantía correspondiente.

Por último y no menos importante, parece necesario discernir entre los delitos de daños y los daños meramente civiles, aunque parece lógico que las principales diferencias residirán, en atención a lo expuesto *supra*, en la intensidad del elemento subjetivo[195], es decir en la concurrencia de una imprudencia leve (puesto que la imprudencia grave sería penalmente relevante en atención al artículo 267 del Código Penal, siendo por ende aplicables para aquellas imprudencias no graves las disposiciones del Código Civil relativas a la responsabilidad extracontractual, en concreto, los artículos 1902 y siguientes

[195] Cfr. GARCIA VALDES, C., MESTRE DELGADO, E., FIGUEROA NAVARRO, C., *op.cit.*, pág. 148.

del Código Civil, en tanto el primero de ellos recoge que *"el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado").*

1.2 Los daños informáticos

Tradicionalmente, venia entendiéndose el daño como un menoscabo, deterioro o destrucción de bienes "materiales"[196], entendiendo como material aquella realidad espacial y perceptible por los sentidos. Sin embargo, con el paso de los años, parece que la doctrina ha tendido a una cierta apertura conceptual (debido quizá a una necesidad de adaptación a los tiempos actuales y al gran auge que ha adquirido la informática), no siendo ya descabellada la idea de entender por daño la afectación o menoscabo, no solo de bienes materiales, sino también de bienes "inmateriales" o "intangibles" como puedan ser los documentos, datos o aplicaciones en soporte informático. No se encuentra sin embargo dicho reconocimiento de la posibilidad del daño sobre bienes intangibles exento de polémica, pues siguen siendo objeto de debate cuestiones como el que ha de considerarse por "daño informático", y la relativa a la determinación del valor de lo destruido, cuyo valor, debido a la naturaleza del objeto del delito, es difícilmente determinable y normalmente bajo[197] en relación con los grandes perjuicios que pueden llegar a ocasionarse con estas conductas[198].

Existe, como ya se adelantaba *supra*, una cierta controversia que rodea a la valoración del daño efectivamente producido dado que rara vez existirá un valor de mercado determinado o ni si quiera se encontrarán a la venta (como es por ejemplo el caso de los documentos y datos, pero no así, en principio, con la mayoría de programas). Autores como FERNANDEZ TERUELO abogan por un criterio de *"coste de recuperación o restablecimiento de la información en el sistema debiendo entender en todo caso colmado el tipo si este no es recuperable o de muy difícil recuperación"*[199], otros autores como GONZALES RUS[200], entienden que han de valorarse en función del

[196] FERNÁNDEZ PALMA, R., MORALES GARCÍA, O., *"El delito de daños informáticos y el caso Hispahack"*, *Diario La Ley*, tomo 1, 2000, pág.3.
[197] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…,* pág. 115.
[198] GARCÍA GARCÍA-CERVIGON, J., *"Daños informáticos. Consideraciones penales y criminológicas", Actualidad Jurídica Aranzadi*, número 588, 2003, pág. 5.
[199] FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…*, pág. 115 y ss.
[200] Cfr. GONZALEZ RUS, J.J, *"Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes"* en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006, pág. 258.

valor estricto que tengan éstos, siendo la conducta irrelevante penalmente en los casos en los que los programas, datos o documentos carezcan de un valor de mercado; por otro lado, otros autores, como FERNÁNDEZ PALMA y MORALES GARCÍA, entienden la necesidad de valoración mediante un criterio más funcional; así, entienden con bastante lógica que, *"en los daños informáticos la valoración del daño debe ser eminentemente funcional, esto es, debe atender a la utilidad concreta de los datos o programas de ordenador. De lo contrario, los desequilibrios de proporcionalidad pueden ser inaceptables, dejando impunes conductas en las que la alteración de datos es insignificante a los efectos del valor del dato en sí y de la capacidad para la recuperación de los mismos, pero que, en el efecto provocado por la alteración (re-programación), se causa un desarreglo de importantes dimensiones económicas"*[201], y sin embargo, tampoco es una solución perfecta, en tanto, se establecería por este método funcional una fina línea entre daño y perjuicio (que será únicamente relevante a efectos de la determinación de la pena y del establecimiento de la correspondiente responsabilidad civil)[202]. En síntesis de lo anterior, parece lógico pensar en la teoría del coste de recuperación como la más apropiada, puesto que, como se analizó en el apartado relativo al tipo básico o tradicional de daños, el perjuicio funciona en los delitos de daños como un mero elemento determinante de la responsabilidad civil postdelictual, siendo necesario puntualizar que, al existir la posibilidad de comisiones imperfectas del tipo, y dada la naturaleza de los datos sujetos a soportes informáticos (siendo manifiesta la facilidad de reproducción y creación de copias de seguridad), habrá de entenderse en aquellos supuestos en los que se produzca un borrado de información y exista una copia de seguridad como un supuesto de comisión en tentativa acabada, cuando el sujeto activo desconozca la existencia de la misma.

Si bien ya se expuso en el apartado anterior la concepción tradicional de daño, habrá de exponerse ahora la concepción de daño informático, entendiendo por aquél, en atención a los artículos 264 y 264 bis del Código Penal, aquella conducta grave y realizada sin autorización consistente, bien en el borrado, daño, deterioro, alteración o supresión que conlleve la inaccesibilidad a datos, programas o documentos informáticos ajenos, o bien en la interrupción u obstaculización en el funcionamiento de un sistema informático ajeno, mediante las conductas ya citadas, mediante la introducción, trasmisión o

[201] FERNÁNDEZ PALMA, R., MORALES GARCÍA, O., *op.cit.*, pág.4.
[202] Cfr. FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos…,* pág. 115 y ss.

destrucción de datos o mediante la destrucción, daño, inutilización, eliminación o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica.

El artículo 264 ter del Código Penal tipifica la producción, adquisición pasa su uso, importación o facilitación por cualquier medio a terceros programas informáticos (concebidos o adaptados para cometer delitos de daños informáticos) o contraseñas de ordenador, códigos de acceso o datos similares que permitan acceder a la totalidad o a parte de un sistema de información, configurándose así este como un tipo de peligro, suponiendo el mismo un adelantamiento de las barreras de protección por el legislador, lo cual se analizará *infra*.

Por último, parece cuanto menos curiosa la discriminación realizada por el legislador entre la documentación en formato físico y la documentación informatizada, no se entiende cómo, por ejemplo, un expediente, se encuentra sujeto a una menor protección en formato papel que en formato digital, siendo escasa o nula la fundamentación del legislador para tal discriminación, máxime cuando en la actualidad la justicia no ha sucumbido a la completa informatización (pese a que en el presente ejemplo, esta conducta pudiera reconducirse igualmente a delito de obstrucción a la justicia). Como bien expone MESTRE DELGADO, *"el Legislador ha estimado – sin mayor justificación- de mayor relevancia que otros bienes susceptibles de daños (por ejemplo, cualquier otro elemento documental en el que se puedan contener los mismos datos contenidos en un soporte informático dañado). Ni el valor de los objetos, ni la modernidad del instrumento de trabajo, son desde luego criterios eficaces para establecer una discriminación punitiva de semejante calibre",* es por ello que sería necesaria o bien una referencia a la destrucción de cualquier tipo de documento, siendo igual la punición independientemente del formato de los mismos, o bien, mediante una restructuración de las penas en el conjunto de delitos de daños en atención a su gravedad, pues no es proporcionado, en este sentido, que la destrucción de forma grave de un documento se equipare prácticamente en su punición a la realización de daños mediante el empleo de sustancias venenosas o corrosivas[203].

[203] Cfr. MESTRE DELGADO, E., *op.cit.*, pág. 414 y ss.

2. Evolución normativa y regulación actual

Previo al análisis de la evolución normativa relativa al daño informático, se hace necesario analizar el Decreto 3096/1973, de 14 de septiembre, por el que se publicaba el Código Penal del año 1973, ya que en su artículo 550 plasmaba la relevancia penal dada a la conducta relativa a la destrucción de documentos, cuando tipificaba que *"el incendio o destrucción de papeles o documentos cuyo valor fuere estimable, se castigará con arreglo a las disposiciones de este capítulo. Si no fuere estimable, con las penas de arresto mayor y multa de 100.000 a 1.000.000 de pesetas"*, siendo con posterioridad y debido a los nuevos avances tecnológicos reformulado completamente para adaptarse a los nuevos tiempos, pero constituyendo uno de los precedentes a la dotación de una cierta relevancia jurídica penal a las conductas tendentes a la destrucción de información plasmada en soportes sujetos a la posibilidad de sufrir daños.

Ya en los años ochenta los ordenadores comenzaban a introducirse en algunos hogares españoles; sin embargo, dada la escasez de los mismos y de la mínima informatización de la sociedad, la delincuencia informática no suponía en un principio demasiada peligrosidad criminal, dado que escasos sectores de población podían permitirse o querían un equipo doméstico. Sin embargo, ello cambio cuando determinadas marcas como Sinclair Research, Commodore International o Amstrad, comenzaron a abrirse paso mediante distribuidores en nuestro país, popularizando la informática en el ámbito doméstico, sobre todo, entre el sector poblacional más joven.

Con la aparición de internet en nuestro país en la década de los noventa, se da un aumento exponencial de la utilización del ordenador tanto en el ámbito laboral como doméstico; así, por ejemplo, es destacable la aparición de sistemas operativos como Windows 95 que permitían un acceso más simple al conjunto de usuarios. Esta progresiva informatización de la sociedad y las posibles oportunidades para los nuevos criminales, llevaron al legislador en el año 1995 a la tipificación, en el artículo 264.2 del Código Penal de 1995, del concepto de daño informático. Así, recogía el precepto que *"la misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos",* siendo la redacción acorde a la época y a las posibilidades de actuación por parte de los cibercriminales. Se adopta finalmente una

solución que difiere bastante de las propuestas de autoras como CORCOY BIDASOLO, que abogaba en el año 1990 por una regulación de estos daños informáticos mediante una reinterpretación y regulación de los delitos de daños e incendios mediante la que pretendía el arreglo de las posibles deficiencias y solucionar las dificultades suscitadas por los daños informáticos[204]. Más adelante, el legislador, en sucesivas reformas, procedió como en algunos países de nuestro entorno más próximo, como se verá en sucesivos párrafos, a la realización de una tipificación independiente de las conductas relacionadas con las nuevas tecnologías, y en concreto, del sabotaje o daños informáticos.

En el año 2001, y tras la ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, quedó clara la postura del Consejo de Europa respecto de la "interferencia de datos" e "interferencia en los sistemas" en tanto en los artículos 4 y 5 del citado texto legal se recogía, respectivamente: *"1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos. 2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves"*, y que *"cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos";* y, si bien en el Código Penal de 1995 ya existía una regulación bastante pareja a la del artículo 4 del citado Convenio, dio base, como se verá en sucesivos párrafos a la modificación del artículo 264 en la reforma operada en el año 2010, introduciendo en el mismo la tipificación de las conductas expuestas por el artículo 5 del Convenio, relativas a la interferencia de los sistemas informáticos.

En el año 2005 se adopta por la Unión Europea la Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, siendo destacables en un primer lugar los artículos 4 y 5 de dicho texto, en tanto exponen que *"cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo,*

[204] CORCOY BIDASOLO, M., *"Protección penal del sabotaje informático. Especial consideración de los delitos de daños"*, *Diario La Ley*, 1990, pág. 15.

transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad", y que *"cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad",* siguiendo así la misma línea que el Convenio de Budapest. Por otro lado, establece la Decisión Marco 2005/222/JAI en los sucesivos preceptos cuestiones relevantes tomadas como base para la modificación del año 2010 de la que se hablará a continuación, tales como la necesidad de introducción de circunstancias agravantes específicas (artículo 7 de la citada Decisión Marco) o bien la necesidad de introducción de responsabilidad penal a personas jurídicas por la realización de las conductas ya citadas (artículo 8 de la citada Decisión Marco).

Posteriormente, y como ya se introdujo *supra*, en el año 2010, siendo la informatización doméstica y social aún mayor (en este sentido, recordar el gráfico correspondiente al uso de internet, expuesto en el apartado *"evolución tecnológica y su impacto en la sociedad: la sociedad de la información y las tecnologías"* correspondiente al marco general de estudio del presente trabajo), y existiendo dispositivos avanzados como *smartphones, tablets* u ordenadores portátiles más potentes y livianos, junto con la aparición de la tecnología 3G que permitían conexión desde prácticamente cualquier parte del territorio y en cualquier momento, se acentúan las posibilidades de los cibercriminales para la ejecución de este tipo de delitos.

Así el legislador, con la aprobación de la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal, y más en concreto, su artículo 67, modifica el artículo 264 en el siguiente sentido: *"1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años. 2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años. 3. Se impondrán las*

penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.º Se hubiese cometido en el marco de una organización criminal. 2. º Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas: a) Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años. b) Multa del doble al triple del perjuicio causado, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33". Así, mientras el Código Penal de 1995 se limitaba a la tipificación de los daños informáticos en un único párrafo, se dedica tras la reforma del año 2010 un precepto completo para dichos comportamientos acorde con la evolución tecnológica a la que se ha hecho referencia con anterioridad. Destacan sobre todo, en este sentido, la inclusión de conceptos como la falta de autorización o la gravedad de la conducta, la obstaculización o interrupción del funcionamiento de sistemas informáticos, la inclusión de supuestos agravados en el artículo 264.3del Código Penal y de penas a las personas jurídicas en el artículo 264.4 del Código Penal.

Posteriormente, en el año 2015, tras la aprobación de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal, en concreto por el artículo 144 de la misma, se realiza no solo una modificación sustancial del artículo 264 del Código Penal, sino que, además, se amplia de forma considerable la tipificación de los daños informáticos mediante la inclusión de los artículos 264 bis, 264 ter y 264 quater del Código Penal.

En lo relativo a las modificaciones realizadas sobre el artículo 264 del Código Penal, el mismo se redacta de la siguiente forma: *"1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.ª Se hubiese cometido en el*

marco de una organización criminal. 2. ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3. ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. 4. ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones. 5. ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero". A grandes rasgos, se limita la modificación a la adición de nuevos supuestos agravados, a la supresión del párrafo relativo a la obstaculización o interrupción del funcionamiento de sistemas informáticos, dado que se dedicará como veremos a continuación un precepto propio, en concreto, el artículo 264 bis del Código Penal, e igualmente, la supresión del párrafo relativo a las penas a las personas jurídicas en tanto también se le dedica un precepto propio, en concreto el artículo 264 quater del Código Penal.

Como ya se adelantó, tras la modificación operada en 2015, se crean nuevos tipos relativos a los daños informáticos, en concreto el artículo 264 bis del Código Penal realiza una tipificación más amplia de la conducta relativa a la obstaculización o interrupción de sistemas informáticos ajenos y en concreto, recoge: *"1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal*

de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero". Así, a diferencia de la redacción del año 2010, se realiza por el legislador una mayor acotación y concreción de las conductas recogidas por el precepto, incluyendo además supuestos agravados como los del artículo 264 bis. 2 y 3 del Código Penal.

Se introduce también en el año 2015 el artículo 264 ter del Código Penal, relativo a la producción, adquisición para su uso, importación o facilitación a un tercero la comisión de daños informáticos mediante programas informáticos, o facilitando contraseñas, códigos o datos similares, y en concreto, expone el tipo que *"será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores: a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información",* si bien es cierto, como puntualiza FARALDO CABANA[205], que el artículo 6 del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, pretende también la represión penal de la elaboración, puesta a disposición y tenencia de dispositivos preordenados para la comisión de daños informáticos sobre datos y sistemas; así, el artículo 6 citado expone que las partes adoptarán medidas para tipificar *"la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de*

[205] Cfr. FARALDO CABANA, P., *"Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio", Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 42/2016, 2016, pág. 19.

cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5”, trasposición que no se ha realizado de una forma fiel al texto, al omitir el legislador español referencia alguna a dispositivos, centrándose el mismo únicamente en programas, contraseñas, códigos de acceso o similares.

Por último, el artículo 264 quater del Código Penal recoge de forma exclusiva la responsabilidad penal de personas jurídicas por la realización de las conductas recogidas por los artículos 264, 264 bis y 264 ter del Código Penal, y en concreto, refiere que *“cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas: a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años. b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33”,* aumentando el precepto el intervalo de las multas imponibles a dichas personas jurídicas.

3. Bien jurídico protegido

Pese a la nula concreción del concepto jurídico daño realizada por el legislador, podría hablarse en un primer momento, al igual que ocurre con el tipo básico de daños, de la protección del bien jurídico patrimonio, puesto que, de realizar un análisis de la ubicación sistemática de los tipos relativos a los daños informáticos (dentro del Código Penal, encuadrándose los mismos dentro del libro II, título XIII, relativo a los delitos contra el patrimonio y contra el orden socioeconómico) y en atención a la propia redacción del tipo, puede determinarse, como ya se expuso la protección del patrimonio, que se entiende menoscabado mediante la pérdida de la funcionalidad o destrucción del objeto material del tipo.

No existe sin embargo un consenso doctrinal en la cuestión relativa a los bienes jurídicos protegidos por los delitos informáticos; por un lado, existe un sector doctrinal, apoyado por autores como ROVIRA DEL CANTO, que entiende la necesidad de una protección de un bien jurídico supraindividual o colectivo por los tipos relativos a los

delitos informáticos, proponiendo así dicho sector diversos bienes jurídicos supraindividuales a proteger, como la seguridad informática, la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, la intimidad informática, la tecnología de internet, la información[206] o la confianza en el correcto funcionamiento de los sistemas informáticos como objeto de tutela penal, también la calidad, pureza e idoneidad de la información contenida en un sistema informático, el software, internet, o la confianza en el correcto funcionamiento de los sistemas informáticos[207], entre otras propuestas. Existe así, por parte de este sector doctrinal, una práctica unanimidad en la existencia de un bien jurídico supraindividual que envuelve a las conductas realizadas mediante o contra sistemas informáticos, discrepando por otra parte en el concreto bien jurídico a proteger. Así, y como ya se adelantaba, ROVIRA DEL CANTO expone que *"con las salvedades propias de toda excepción a la regla, la punibilidad debe venir determinada, en este ámbito, por la potencialidad de las conductas o comportamientos en afectar gravemente la información en sí misma como bien jurídico supra individual y el interés colectivo en la seguridad y fiabilidad de los sistemas y redes de almacenamiento, tratamiento, procesamiento y transferencia de la misma, siendo por tanto el método a utilizar el de formulación de tipos delictivos de riesgo abstracto en cuanto a la grave afectación de estos nuevos bienes jurídicos, con independencia del requerimiento por alguna figura concreta, además y en su caso, de un resultado perjudicial, lesivo o dañino de un bien jurídico tradicional, individual o colectivo también protegido y recurrente"*[208]. Esta corriente doctrinal defensora de la existencia de un bien jurídico supraindividual (que han de proteger los tipos relativos a los delitos informáticos), mantiene cierto deje iusnaturalista al parecer entender, como expone GUTIÉRREZ FRANCÉS cuando reflexiona sobre el bien jurídico, que *"el Legislador, por tanto, no lo inventa, sino que lo encuentra en la realidad social, en cada grupo social concreto, y dentro de cada concreto –también- momento histórico. El bien jurídico no es, pues, una categoría formal, sino que está dotado de un contenido material irrenunciable, asentado en la vida social misma y sin el cual no existe, aun cuando siga utilizándose su nombre"*[209], es decir, que parecen entender que, llegados a este contexto social, en el que la tecnología y la informática se han transformado en un imprescindible,

[206] HERNÁNDEZ DÍAZ, L., *op.ci.*, págs. 237 y ss.
[207] MAYER LUX, L., *"El bien jurídico protegido en los delitos informáticos", Revista Chilena de Derecho*, volumen 44, número 1, 2017, págs. 240 a 244.
[208] ROVIRA DEL CANTO, E., *op.cit.*, págs. 73 y 74.
[209] GUTIERREZ FRANCES, M.L., *op.cit.*, pág. 202.

se requiere de la protección de nuevos bienes jurídicos supraindividuales como la seguridad informática.

Por otro lado, se posiciona otro sector doctrinal, al que pertenecen autores como FARALDO CABANA o DE LA MATA BARRANCO, en una postura más conservadora, al entender que en estos delitos se realiza una protección coincidente por lo general con la de los tipos tradicionales, siendo estos, una mera forma del legislador de adaptarse a nuevas formas de comisión o bien debiéndose ello a la aparición de nuevos supuestos que los tipos tradicionales no abarcan con precisión. Así merece la pena citar a DE LA MATA BARRANCO cuando expone que *"no existe en nuestro texto legal -cuyo acertado criterio de sistematización de los diferentes delitos es, básicamente, el del bien jurídico afectado por cada uno de ellos-, ni un Capítulo dedicado a los delitos informáticos, ni un concepto de delito informático, ni un listado de conductas vinculado a este tipo de criminalidad"*[210], o a FARALDO CABANA, cuando afirma que, *"en este proceso de adaptación de los delitos clásicos hay que destacar, en particular, la inexistencia de un bien jurídico supraindividual o colectivo que pueda identificarse con la seguridad informática, o algún concepto semejante"*[211].

4. Elementos de la punición

4.1 Ejecución

El delito de daños informáticos se configura como un delito de resultado en tanto se distingue perfectamente, en su configuración legal, una acción típica, causante del daño concreto, y un resultado, consistente en un manifiesto menoscabo, detrimento o destrucción del objeto material del delito que ocasiona un perjuicio económico en el propietario del bien dañado y que no se ve en principio compensado con un correlativo enriquecimiento directo del sujeto activo, dado que la conducta típica consiste, como se adelantaba, en la destrucción o merma de su valor[212].

[210] DE LA MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L., *"Los delitos vinculados a la informática en el derecho penal español (parte I)"* en *Derecho Penal Informático*, Civitas, España, 2010, págs. 159 y ss.
[211] FARALDO CABANA, P., *"Estrategias legislativas…"*, págs. 1 y 2.
[212] Cfr. MESTRE DELGADO, E., *op.cit.*, pág. 411.

En atención a la anterior afirmación, pueden distinguirse en este tipo de delitos diversas fases de ejecución (salvo en el caso del artículo 264 ter, que, al configurarse como un delito de peligro, se consuma sin necesidad de lesión efectiva, es decir, se consuma con la simple puesta en peligro del bien jurídico, siendo posible únicamente la apreciación de la tentativa inacabada), siendo por ello apreciable tanto la tentativa inacabada como acabada. Concurrirá la tentativa inacabada cuando el sujeto interrumpa de forma involuntaria la acción delictiva sin haber realizado el conjunto de actos ejecutivos necesarios para la consecución del resultado dañoso. Por otro lado, concurrirá la tentativa acabada cuando el sujeto, realizando el conjunto de dichos actos ejecutivos necesarios para la consecución del resultado, no logre su producción por causas ajenas al mismo.

Respecto a la consumación del tipo de daño informático, no entraña demasiada duda, puesto que la consumación se apreciará cuando se produzca de forma efectiva el resultado típico, es decir, la causación efectiva del daño, menoscabo, detrimento o destrucción del objeto material del tipo.

Respecto a la posibilidad de comisión activa u omisiva, por interpretación conjunta de los artículos 10 y 11 del Código Penal, cabe rechazar la posibilidad de apreciación de supuestos de omisión pura o propia, en tanto no se tipifica la misma respecto del daño informático, es decir, a tenor de lo dispuesto por el artículo 10 del Código Penal (*"son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley"*), se exige su expresa tipificación, cosa que no ocurre en este tipo de delitos. Por otra parte, no existen dudas de la posibilidad de comisión activa o por acción. Sin embargo, como bien puntualiza ROVIRA DEL CANTO[213], las expresiones empleadas por el legislador y la apertura conceptual de las mismas permiten admitir posibilidad de apreciar la comisión por omisión; así, el legislador, al emplear expresiones como *"el que por cualquier medio"*, hace pensar en la posibilidad de apreciación de dicha figura recogida por el artículo 11 del Código Penal. En concreto, dicho precepto dispone que *"los delitos que consistan en la producción de un resultado sólo se entenderán cometidos por omisión cuando la no evitación del mismo, al infringir un especial deber jurídico del autor, equivalga, según el sentido del texto de la ley, a su causación. A tal efecto se equiparará la omisión a la acción: a) Cuando exista una específica obligación legal o*

[213] ROVIRA DEL CANTO, E., *op.cit.*, pág. 235.

contractual de actuar. b) Cuando el omitente haya creado una ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente", no siendo difícil imaginar un caso de daños informáticos perpetrado de tal forma, por ejemplo, la no introducción intencionada de determinados datos o comandos por parte del informático de la empresa que interrumpen el funcionamiento normal del sistema o producen el borrado de los datos contenidos en el mismo, o bien la observación por éste de malware o posibles amenazas inminentes para el tejido informático empresarial y no actuar el mismo pues sabe que, de no actuar, se producirán daños informáticos.

Por otro lado, en atención al artículo 267 del Código Penal, puede apreciarse la comisión imprudente de este tipo de delitos; sin embargo, el precepto expone que *"los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos. Las infracciones a que se refiere este artículo sólo serán perseguibles previa denuncia de la persona agraviada o de su representante legal. El Ministerio Fiscal también podrá denunciar cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida. En estos casos, el perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130 de este Código",* es decir, que solo será punible la imprudencia grave, despenalizando las imprudencias menos graves y las leves, que de por sí, ya se encontraban despenalizadas en virtud de los principios de ultima ratio y de intervención mínima del Derecho penal, como se desprende del preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, más concretamente en su apartado XXXI, cuando refiere que *"se recoge así una modulación de la imprudencia delictiva entre grave y menos grave, lo que dará lugar a una mejor graduación de la responsabilidad penal en función de la conducta merecedora de reproche, pero al mismo tiempo permitirá reconocer supuestos de imprudencia leve que deben quedar fuera del Código Penal. No toda actuación culposa de la que se deriva un resultado dañoso debe dar lugar a responsabilidad penal, sino que el principio de intervención mínima y la consideración del sistema punitivo como última ratio, determinan que en la esfera penal deban incardinarse exclusivamente los supuestos graves de imprudencia, reconduciendo otro tipo de conductas culposas a la vía civil, en su modalidad de responsabilidad extracontractual o aquiliana de los artículos 1902 y*

siguientes del Código Civil, a la que habrá de acudir quien pretenda exigir responsabilidad por culpa de tal entidad". Además, el Tribunal Supremo, en la STS 722/1999, de 6 de mayo [214], expone que *"cuando es el patrimonio, solamente se protege penalmente en función del daño, con evidentes e irritantes discriminaciones. Más se olvida que el artículo citado responde a lo que las exigencias del principio de mínima intervención imponen en aquellos casos en los que el daño causado sea menor. Ello sin embargo no supone que por debajo de las cuantías mínimas exigidas se declare que la imprudencia no es antijurídica, sino que, simplemente, se declara la misma fuera de la intervención penal, por razones político criminales y no por carencia de «injusticia». De ahí que se pueda ejercitar una acción civil en reclamación del perjuicio sufrido cuando es inferior a los diez millones establecidos por la ley".* Es decir, que solo serán punibles como delitos imprudentes de daño informático aquellos supuestos en los que se superen los 80.000 euros, siendo posible la apertura del procedimiento a instancia del ofendido (o su representante legal) o por el Ministerio Fiscal (cuando el ofendido sea menor de edad o persona discapacitada necesitada de especial protección), siendo aceptable el perdón del ofendido para la extinción de la acción penal. Así, se establece una barrera que permite discernir cuándo los daños tendrán relevancia penal, o bien, únicamente civil en atención a la intensidad de la culpa, es decir, siendo daños civiles aquellos actos cometidos por imprudencia, salvo aquellos en los que concurra una imprudencia grave en una cuantía superior a los 80.000 euros.

Respecto a los actos preparatorios, no serán penalmente relevantes las conductas relativas a la provocación, conspiración y proposición, como sí ocurría, por ejemplo, en los delitos de estafa informática por aplicación del artículo 269 del Código Penal, pues, por previsión de los artículos 17 y 18 del Código Penal, serán éstos únicamente punibles en los casos expresamente previstos por la ley, no haciéndose referencia expresa respecto de los tipos de daños informáticos.

Tras la introducción en el año 2015 del artículo 264 ter, como ya se adelantaba, se produce por el legislador un adelantamiento de las barreras de protección[215], configurándose así el tipo de peligro, los cuales *"se consuman sin necesidad de lesión, con el simple peligro […] del bien jurídico, suponiendo por tanto un adelantamiento de*

[214] Cfr. MESTRE DELGADO, E., *op.cit.*, pág. 419.
[215] GALAN MUÑOZ, A., *"El nuevo delito del artículo 248.2 CP…"*, pág. 2.

las barreras de protección a una fase anterior a la lesión"[216], y si bien se podría entender la necesidad del tipo para aquellos supuestos en los que el sujeto se limita a la creación o distribución de las herramientas (programas, contraseñas, códigos de acceso o datos similares) en calidad intermediario, no se entendería la punición para aquellos casos en los que el sujeto que dispone de las capacidades para crear por sí mismo dichas herramientas, las emplea además para la comisión del delito de daños informáticos, siendo así la conducta en el caso de los sujetos que adquieren, producen o importan las herramientas para ser posteriormente utilizadas por ellos para la comisión de los daños informáticos meros actos preparatorios para la realización del delito de daños, entendiendo contraria al principio *non bis in ídem* la apreciación de cualquier tipo de punición conjunta entre el artículo 264 ter junto con los artículos 264 o 264 bis cuando el sujeto adquiera o cree una herramienta para realizar los daños informáticos por sí mismo, sin distribuir de forma separada dicha herramienta, en tanto se produciría una absorción de la conducta por los artículos 264 y 264 bis del Código Penal.

Por otro lado, parece lógico que el sujeto que se dedica a la distribución, producción o importación de este tipo de herramientas, pueda incurrir no solo en delitos de daños propiamente dichos, sino que, además, pueda comerciar de forma paralela con este tipo de herramientas con el ánimo de lucrarse; sin embargo, una posible consecuencia de la tipificación independiente de este tipo de actos preparatorios (o de facilitación) sea una desvirtualización de la figura del cooperador necesario; quizá, de no existir el artículo 264 ter del Código Penal, dicha conducta sería perfectamente reconducible a esta forma de participación delictiva.

4.2 Autoría y participación

Son de perfecta aplicación a los delitos de daños informáticos los artículos 28 y 29 del Código Penal relativos a la autoría y participación, si bien cabe destacar que se considerarán autores de un delito de producción, adquisición para su uso o para su facilitación a terceros de programas informáticos, contraseñas, códigos de acceso o datos similares para facilitar la comisión de delitos de daños informáticos, y no como participes de éstos a los sujetos que realicen las conductas antes citadas y recogidas por el artículo 264 ter. Además se prevé por el legislador, según lo recogido por el artículo 264 quater

[216] LUZÓN PEÑA, D.M., *op.cit.*, pág. 169.

del Código Penal, en relación con el artículo 31 bis del Código Penal, la autoría de estas conductas por personas jurídicas[217].

4.3 Circunstancias

Son de aplicación al tipo de daño informático la gran mayoría de circunstancias atenuantes y agravantes recogidas en el Código Penal; en este sentido, dada la propia redacción del artículo 22.1º del Código Penal cuando expone que *"hay alevosía cuando el culpable comete cualquiera de los delitos contra las personas",* se entiende la inaplicabilidad de dicha circunstancia agravante al ser un delito inminentemente patrimonial. Por otro lado, pese a que no se desprende de forma literal del propio precepto, como en el caso anterior, puede entenderse de igual manera inaplicable la agravación del artículo 20.5º del Código Penal, relativa al ensañamiento, puesto que difícilmente se podrá, en un delito de carácter patrimonial (como es el tipo de daños informáticos), aumentar deliberada e inhumanamente el sufrimiento de la víctima. Respecto de la circunstancia mixta de parentesco, será de aplicación en virtud de lo dispuesto por el artículo 268 del Código Penal como eximente de responsabilidad criminal siempre que no concurra violencia, intimidación, abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad.

4.4 Penalidad

Se mantendrá en el presente apartado una estructura argumentativa acorde a la dispuesta por el Código Penal. Así, se recoge por el artículo 264.1 del Código Penal el tipo básico de daño informático con una pena de prisión de seis meses a tres años.

Existen respecto al mismo, modalidades o formas agravadas; así, se recoge por el artículo 264.2 del Código Penal una pena de prisión de dos a cinco años y multa del tanto al duplo cuando concurran determinadas circunstancias (comisión en el marco de una organización criminal, cuando se produzcan daños de especial gravedad o afectando a un número elevado de sistemas informáticos, ocasionar un perjuicio grave en el funcionamiento de servicios públicos esenciales o en la provisión de bienes de primera necesidad, cuando afecte al sistema informático de una infraestructura crítica o se hubiera

[217] MESTRE DELGADO, E., *op.cit.*, pág. 368.

creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea, o de un Estado Miembro de la misma y cuando se hubieran utilizados los medios referidos por el artículo 264 ter). Igualmente, de resultar los hechos de extrema gravedad, se prevé por el precepto que podrá imponerse la pena superior en grado.

Y no solo eso, dado que se prevé por el artículo 264.3 del Código Penal la imposición de las penas recogidas por los artículos 264.1 y 2 del mismo texto en su mitad superior, cuando los hechos se hubieren cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Por otro lado, el tipo básico de interrupción u obstaculización de sistemas informáticos, tipificado en el artículo 264 bis.1 del Código Penal, recoge una pena de prisión de seis meses a tres años. Respecto a las modalidades agravadas, se impondrá la citada pena en su mitad superior cuando los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública. Respecto de dichas modalidades agravadas, se recoge por el artículo 264 bis. 2 del Código Penal una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando se realicen las conductas del artículo 264 bis.1 y concurra además alguna de las circunstancias recogidas por el artículo 264.2 del Código Penal. Cuando las conductas recogidas por el artículo 264 bis.1 y 2 del Código Penal hubieran sido cometidas mediante la utilización de ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero, se impondrá la pena en su mitad superior.

Respecto del tipo básico que podríamos llamar de facilitación o preparación, del artículo 264 ter del Código Penal, se castigará el mismo con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses.

Para el caso de que fuere una persona jurídica la responsable de los delitos recogidos por los artículos 264, 264 bis y 264 ter del Código Penal, se le impondrá una pena de multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años, o multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. Igualmente, podrán los jueces y tribunales imponer las penas recogidas en las letras b) a

g) del apartado 7 del artículo 33, en atención a lo dispuesto por el artículo 66 bis del Código Penal.

Respecto a la posibilidad de apreciación de continuidad delictiva, si bien parece plausible y no se descarta en atención a los medios empleados para la ejecución (sistemas informáticos que permiten la realización de un sinfín de acciones de forma automática), y pareciendo en principio aplicable el artículo 74 del Código Penal para aquellos supuestos en los que el sujeto realice las conductas mediante un plan preconcebido o aprovechando idéntica ocasión (imagínese por ejemplo, un programa, como pueda ser un virus o un gusano informático, que es introducido subrepticiamente en la memoria de una computadora y que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada), realice una pluralidad de acciones que ofendan a uno o varios sujetos e infrinjan el mismo precepto penal o preceptos de igual o semejante naturaleza, difícilmente podrá ello extrapolarse a supuestos fuera de laboratorio. Así, en el caso de los artículos 264 y 264 bis del Código Penal, que recogen ya en su propia redacción supuestos en los que se afecta a un número elevado de sistemas informáticos, no es posible su entendimiento en virtud del principio *non bis in ídem*. Por otro lado, nada se dice respecto al artículo 264 ter del Código Penal, siendo en este caso perfectamente viable la aplicación de la continuidad delictiva; así, por ejemplo, parece ello viable para el caso en el que el sujeto se dedique a la venta de programas o códigos mediante una tienda en la Deep Web, siendo el procedimiento por el que se realiza la transacción completamente automático. De entender la concurrencia de la figura de la continuidad delictiva, para el caso de delitos contra el patrimonio, y en atención a lo dispuesto por el artículo 74.2 del Código Penal, se impondrá la pena en atención al perjuicio total causado, pudiendo el juez de forma motivada imponer una pena superior en uno o dos grados en la extensión que estime conveniente cuando el hecho revistiere una notoria gravedad o hubiere perjudicado a una generalidad de personas.

En materia de concursos, cabe destacar que no se desprecia la posibilidad de entender concurrentes las figuras del concurso real de delitos, recogido por el artículo 73 del Código Penal, y del concurso medial (del todo habitual en delitos informáticos, donde se encadenan infracciones necesarias para cometer otras) recogido por el artículo 77.1 y 3 del Código Penal, siendo además este último de lo más habitual, dada la dinámica seguida por los ciberdelincuentes, que normalmente no limitan su actuación a la comisión de un único delito informático. Así, por ejemplo, no es extraño imaginar al cibercriminal

introduciéndose de forma ilícita en el sistema informático ajeno a través de un troyano (malware que toma la apariencia de un programa legitimo) o aprovechando vulnerabilidades del sistema, tomando el control del mismo, extrayendo cuantos datos guste para posteriormente dañarlo por completo, pudiendo llegar finalmente incluso a extorsionar a los usuarios mediante la información obtenida, o instalando programas que hacen uso de la potencia de procesamiento del sistema para obtener beneficios. Suscita sin embargo ciertas dudas la figura del concurso ideal de delitos recogida por el artículo 77.1 y 2 del Código Penal. Así, dada la redacción realizada por el legislador, será cuanto menos difícil la apreciación de un concurso ideal de delitos, para el que se requiere de un solo hecho que constituya dos o más delitos, no excluyéndose sin embargo la posibilidad de su concurrencia pese a la dificultad en su apreciación. Por ejemplo, pese a que en una supresión de datos del artículo 264 del Código Penal, que afectare u obstaculizare el funcionamiento del sistema informático del artículo 264 bis del Código Penal, pudiera parecer clara la concurrencia de un concurso ideal de delitos, es el propio Código Penal el que suprime dicha posibilidad al recoger el artículo 264 bis que *"será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior"*.

4.5 Responsabilidad civil

Será de aplicación el título V, del libro I, del Código Penal; sin embargo, pueden destacarse los artículos 109.1 (en cuanto dispone que *"la ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados")* y 110 del Código Penal (relativo a la extensión de la responsabilidad civil). No debe olvidarse tampoco por su relevancia el artículo 116 del Código Penal, cuando expone que *"toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que deba responder cada uno"*, también que *"los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables"*, y que *"la responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil*

en los términos establecidos en el artículo 110 de este Código de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos".

5. Elementos del tipo

Respecto a la acción típica, consistirá la misma, en atención al tenor literal de la legislación, en la realización de cualquier conducta encaminada a causar un daño, en concreto, para el caso del artículo 264.1 del Código Penal, "*por cualquier medio, sin autorización y de manera grave"*, es decir, que la acción para este caso es ciertamente indeterminada, y por otro lado, el artículo 264 bis del Código Penal recoge que consistirá la acción en la realización de las conductas recogidas por el artículo 264 del Código Penal (introducción o transmisión de datos, o bien, destrucción, daño, inutilización, eliminación o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica). Exigiéndose para ambas la necesidad de concurrencia del carácter grave de la conducta y su realización sin la correspondiente autorización.

Respecto del objeto material del delito, en el caso del artículo 264 del Código Penal, comprenderá los datos informáticos, programas informáticos o documentos electrónicos, mientras que, para el caso del artículo 264 bis del Código Penal, comprenderá en principio el sistema informático en su totalidad. Si bien no entraña duda, por la redacción realizada por el legislador, la configuración del *software* como objeto material del delito, es decir, del soporte lógico del sistema, haciendo referencia en este caso al conjunto de programas, instrucciones y reglas informáticas (así, por ejemplo, el sistema operativo, programas y aplicaciones, entre otras) que hacen uso del hardware para funcionar y que son intangibles en tanto no existen en el plano físico, cabría cuestionarse sin embargo, si el *hardware* o soporte físico de los datos, es decir, el conjunto de los componentes físicos de los que se consta el equipo (procesador, batería, fuente de alimentación, placa base, tarjeta gráfica, memoria RAM, discos duros, entre otra serie de componentes) configuraría el objeto material del delito. La respuesta será afirmativa, si se entiende por sistema informático el conjunto del sistema, es decir, la conjunción de *hardware* y *software*. Así, se entiende en el presente trabajo una concepción no restrictiva de sistema informático en los términos anteriormente expuestos, pues ello es perfectamente plausible dada la redacción de los artículos 264 y 264 bis del Código Penal; en este sentido, el primero de los artículos citados emplea una formula ciertamente abierta

(“*por cualquier medio”)* mediante la cual no cabe despreciar la posibilidad de daño al *hardware* como soporte físico de los datos, programas o documentos electrónicos protegidos por el tipo; así, por ejemplo, la desmagnetización de un disco duro que conllevaría la pérdida de la información contenida en el mismo (debe recalcarse que, para el caso del artículo 264 del Código Penal, será únicamente encuadrable aquel daño en el *hardware* que provoque daños a datos, programas o documentos electrónicos protegidos por el tipo), y por otro lado, el segundo de los artículos citados, al exigir la obstaculización o interrupción del funcionamiento del sistema, y al emplear en su redacción fórmulas como *“realizando alguna de las conductas a que se refiere el artículo anterior”* o *“destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de datos”*, permiten perfectamente entender subsumible en el tipo aquella conducta tendente a la destrucción de componentes físicos, *hardware,* que implique un resultado prohibido por el tipo (obstaculización o interrupción del sistema); así, por ejemplo, el sujeto que en una central nuclear destruye la placa base del panel central de mandos del reactor que provoca una interrupción del funcionamiento normal del mismo.

En síntesis, en atención al tenor literal de estos preceptos, y dadas las expresiones empleadas por el legislador, cabría un encuadre de ataques a elementos físicos (como fueren el quemar el componente o hacer uso de imanes para su alteración) o a elementos lógicos (mediante el uso de vulnerabilidades del sistema, programas o cualquier proceso lógico o físico), siempre que exista una gravedad y una realización de la conducta sin la correspondiente autorización y ocasione daños a la información o afecten al funcionamiento normal del sistema informático. Además, tampoco sería en la mayoría de los casos de aplicación el artículo 263 del Código Penal, en tanto el artículo 264 bis del Código Penal, como se verá en sucesivos apartados, tipifica la obstaculización o interrupción de forma grave de sistemas informáticos, es decir, que de producirse un daño grave sobre los componentes físicos que ocasionaren interrupciones u obstaculizaciones en el funcionamiento del sistema, como por ejemplo atacando a la placa base; habría de encuadrarse aquella conducta en el citado precepto en atención a lo dispuesto por el artículo 8 del Código Penal, siendo reconducible únicamente el ataque a elementos físicos del sistema informático al delito tradicional de daños cuando de la conducta no se ocasionen daños a la información o afecten al funcionamiento normal del sistema

informático, pues no concurrirían los elementos de los tipos correspondientes a la punición del daño informático.

Respecto del resultado típico, consiste el mismo en el borrado, daño, deterioro, alteración o supresión que conlleve la inaccesibilidad a datos, programas o documentos informáticos ajenos, o bien en la interrupción u obstaculización en el funcionamiento de un sistema informático ajeno, mediante las conductas del artículo 264 del Código Penal, mediante la introducción, trasmisión o destrucción de datos, bien mediante la destrucción, daño, inutilización, eliminación o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica.

6. Formulas específicas

6.1 Daños sobre el hardware que afectan al sistema o al software

Entre otras muchas, incendio de instalaciones o de equipos, explosión de bombas, golpes de martillo, uso de imanes, vertiendo líquidos, o mediante el uso de técnicas más avanzadas y menos arriesgadas, como el uso del famoso "*USB killer 2.0"*, una unidad de almacenamiento portátil capaz de conectarse al equipo mediante el puerto USB, almacenando parte de la energía del equipo en condensadores para posteriormente descargar toda la carga almacenada en la placa base de la computadora o del equipo en cuestión, *"quemando",* es decir, sobretensando (fenómeno conocido vulgarmente como pico de tensión) el equipo en escasos segundos. Caso habitual también es el de la destrucción de los discos duros destruyéndolos en trituradoras o mediante otras técnicas como el uso de desmagnetizadores, dado que el procedimiento de borrado de los mismos no es irreversible, pudiendo recuperarse en la mayoría de los casos información de los mismos.

Debido al infinito número de conductas posibles, se hace necesario sintetizar a fin de no enfangar el presente TFM. Baste con entender por daños sobre el hardware aquellas conductas que, si bien se asemejan al concepto clásico de daños, en cuanto se realizara un ataque físico sobre elementos tangibles o bienes materiales, como son los elementos que configuran el hardware del sistema informático, son encuadrables dentro del tipo de daño informático en cuanto la conducta se realiza con el fin, no de destruir el componente físico en sí, sino que busca dañar al software y con ello, el borrado, daño, deterioro,

alteración o supresión que conlleve la inaccesibilidad a datos, programas o documentos informáticos ajenos, o bien la interrupción u obstaculización en el funcionamiento de un sistema informático ajeno.

6.2 Daños sobre el hardware mediante acciones del software

En la actualidad, se podría decir que no es viable una afección directa del hardware mediante software, sin embargo, sí es posible por ejemplo mediante software hacer que las piezas de unidades de almacenamiento o discos duros mecánicos se muevan a grandes velocidades buscando un temprano desgaste o rotura de las mismas, el aumento de la temperatura por un incremento de la potencia de procesamiento que desgasta o daña prematuramente ciertos componentes (como en el *cryptojacking*), o bien la introducción y borrado de datos continua y rápida en unidades de estado sólido, buscando "quemar" las celdas, dado el limitado ciclo de escritura del que gozan las mismas.

Por otro lado, y si bien es cierto que solo se mencionará como mera curiosidad, no se encuentra el hardware, pese a que así lo pareciera a simple vista, exento de vulnerabilidades (que no pueden ser subsanadas vía actualización como el software)[218].

6.3 Daños al software mediante software

Son aquellos en los que el legislador centra mayor atención conforme a la redacción de los tipos ya expuestos. Así, existen innumerables formas de dañar el software o elementos lógicos del sistema mediante procedimientos puramente informáticos o lógicos con el objetivo de provocar el borrado, daño, deterioro, alteración o supresión que conlleve la inaccesibilidad a datos, programas o documentos informáticos ajenos, o bien la interrupción u obstaculización en el funcionamiento de un sistema informático ajeno.

En los sucesivos apartados se expondrá una serie de fórmulas específicas sin ser dicha exposición de naturaleza *numerus clausus*, existiendo un sinfín de fórmulas que no se expondrán en aras de una cierta sintetización del presente trabajo. Baste así con

[218] https://cso.computerworld.es/tendencias/cuales-son-las-principales-amenazas-de-seguridad-para-el-hardware (consulta 2 de enero de 2019).

mencionar ciertas formulas específicas relevantes para la ejemplificación de lo expuesto en la presente sección.

Así, una de las fórmulas más populares de ataque es la del uso de *malware* o *software* malicioso, es decir, un tipo de *software* cuyo objetivo consiste en la infiltración en el sistema informático para perturbar su normal funcionamiento, controlar o dañar al mismo o la información que en él se contiene. Sin embargo, la terminología de *malware* engloba en su seno un gran número de *software* malicioso. Pueden destacarse así dentro del *malware*[219] a los virus informáticos, los cuales son programas informáticos que se reproducen a sí mismos, contaminando otros programas (como si de células huésped se tratasen) y que son capaces de generar un daño ya no solo al sistema informático, sino a la información almacenada en el mismo. Como bien expone ANDRES DOMINGUEZ en el sentido de lo anterior, *"puede destruir no solo rutinas y datos, sino que combinado con bombas lógicas activado al mismo tiempo o con posterioridad infecta el sistema completo e incluso las copias de seguridad. Provoca una mayor lentitud en la ejecución de programas […], la desaparición de informaciones del disco duro"*[220]. Por otro lado, son igualmente comunes los gusanos informáticos que, al igual que el virus, tienen capacidad de duplicarse a sí mismos aprovechando la automatización del sistema informático y que, a diferencia de éstos, puede propagarse a diferentes sistemas informáticos por medio de redes informáticas; además, no requieren como los virus (para su transmisión) de la concurrencia de una acción humana y tampoco de un archivo soporte o huésped. Los troyanos son igualmente un tipo de *malware* que, con la apariencia de un *software* legítimo, se introducen en el sistema y permiten al sujeto acceder al sistema para borrar, modificar datos, interrumpir el funcionamiento normal del sistema, entre otras funciones.

Son igualmente comunes los ataques de denegación de servicio mediante redes de ordenadores *zombie* o *botnets*[221], es decir, redes de equipos controlados a distancia, mediante el uso de malware para tomar el control de sistemas informáticos, denominando a los dispositivos controlados como *bots* o z*ombies*, también mediante el uso de *rootkits*, mediante los que se pretende igualmente tomar el control del sistema sin consentimiento de sus titulares, y que son empleados habitualmente para atacar páginas web o servidores

[219] MIRO LLINARES, F., *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons Ediciones Jurídicas y Sociales, Madrid, 2012, pág. 59 y ss.
[220] ANDRÉS DOMÍNGUEZ, A., *"Los daños informáticos en la Unión Europea"*, *Diario La Ley*, tomo 1, 1999, pág. 3.
[221] Cfr. FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso…",* págs. 363 y ss.

mediante la creación de grandes cantidades de tráfico a las mismas, "tumbándolas", es decir, inhabilitándolas por completo, con el consiguiente daño producido, siendo un claro ejemplo de ello la red cibercriminal "mariposa", la cual controlaba millones de ordenadores para estos fines[222].

Sección 4ª: Delitos contra la propiedad intelectual, la piratería informática

1. Concepto y denominación

Define la RAE, quizá de forma excesivamente escueta desde un punto de vista jurídico, la propiedad intelectual como el derecho de explotación exclusiva sobre las obras literarias o artísticas que la ley reconoce a su autor durante un cierto plazo. Sin embargo, como bien recoge por el artículo 20.1.b) de la Constitución española, se reconocen y protegen los derechos de *"producción y creación literaria, artística, científica y técnica"*, siendo así, objeto de protección constitucional, no solo la creación literaria o artística, sino también, la producción y creación científica y técnica. Ciertos autores, sin embargo, entienden la misma más como una manifestación del derecho a la propiedad recogido por el artículo 33.1 de la Constitución española[223] que como el derecho a la producción y creación anteriormente expuesto; sin embargo, en aras de no extender innecesariamente el presente trabajo, se analizarán cuestiones de mayor relevancia para el mismo.

Como bien se recoge en el apartado XVII de la Ley Orgánica 1/2015, de 30 de marzo, la Ley de Propiedad Intelectual es el instrumento de protección natural en dicha materia y, como tal, se dependerá de la misma como pilar básico para el desarrollo y regulación de la citada materia.

Una vez expuesto lo anterior, no será extraño que surjan dudas sobre qué elementos se engloban dentro de la terminología *"producción y creación literaria, artística, científica y técnica";* a este fin, se hace imprescindible la alusión a los artículos 10 a 12 de la Ley de Propiedad Intelectual, en tanto en los mismos se realiza una recopilación de carácter *numerus apertus* sobre aquellas creaciones objeto de propiedad intelectual. Establece así el artículo 10 que *"son objeto de propiedad intelectual todas las*

[222] https://elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html (Consulta 6/12/2018).
[223] FAYOS GARDÓ, A. *"La propiedad intelectual tras la ley 21/2014", Editorial La Ley*, Actualidad Civil, 2015, pág. 1.

creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza. b) Las composiciones musicales, con o sin letra. c) Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales. d) Las obras cinematográficas y cualesquiera otras obras audiovisuales. e) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o comics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas. f) Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería. g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia. h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía. i) Los programas de ordenador" y *"el título de una obra, cuando sea original, quedará protegido como parte de ella*". Por otro lado, el artículo 11 recoge que *"sin perjuicio de los derechos de autor sobre la obra original, también son objeto de propiedad intelectual: 1.º Las traducciones y adaptaciones. 2.º Las revisiones, actualizaciones y anotaciones. 3.º Los compendios, resúmenes y extractos. 4.º Los arreglos musicales. 5.º Cualesquiera transformaciones de una obra literaria, artística o científica"*. Y finalmente, el artículo 12.1 del mismo texto, dispone que *"también son objeto de propiedad intelectual, en los términos del Libro I de la presente Ley, las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos"*, que serán englobadas en aras de facilitar la redacción del presente trabajo como "obras".

Son así objeto de protección por la propiedad intelectual, como bien recoge la ley, aquellas creaciones expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro. Sin embargo, se hace necesario destacar el artículo 10.1.i) de la Ley de Propiedad Intelectual, en cuanto reconoce como objeto de protección a los programas informáticos, definiéndose los mismos por el artículo 96 del mismo texto como *"toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera*

que fuere su forma de expresión y fijación", y, en segundo lugar, las bases de datos, recogidas, como se vio, por el artículo 12.1, y definidas por el artículo 12.2 y 3 de la Ley de Propiedad Intelectual, que en concreto expone que *"se consideran bases de datos las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma",* y que *"la protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos",* limitándose así el ámbito de protección de las bases de datos a las mismas en *stricto sensu*, quedando los programas protegidos de la forma ya expuesta anteriormente.

Destacable igualmente en este sentido será el Convenio de Budapest de 23 de noviembre de 2001 sobre la ciberdelincuencia, en concreto, su artículo 10, cuando regula los delitos informáticos contra la propiedad intelectual, enmarcándolos dentro de la categoría de delitos *"relacionado con el contenido"* y dentro de ella como *"delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines",* hecho que parece haber conducido a diversos autores, como VELASCO NUÑEZ[224], a entender que este tipo de delitos no son propiamente informáticos, pero en los que cabe una comisión a través de Internet. Quizá pueda ello deberse a la clasificación realizada por el citado Convenio, en tanto en su clasificación distingue entre *"delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"*, *"delitos informáticos"* y "*delitos relacionados con el contenido".* Ello conduce a cuestionarse nuevamente ¿qué es un delito informático? Pues bien, siguiendo la tesis expuesta en el apartado relativo al marco de estudio general del presente trabajo, bajo el título de *"delito informático: concepto, características y tipología"*, se expone la posibilidad de una adopción estricta o restrictiva del término "delito informático", la cual parece adoptar el citado sector doctrinal, y que se rechaza en el presente trabajo, entendiendo por ende el mismo en sentido amplio.

2. Evolución normativa y regulación actual

En el año 1985 se firmó por España el Acta de Adhesión de España a las Comunidades Europeas; años después de este hecho, se adoptaron por las entonces

[224] Cfr. VELASCO NÚÑEZ, E., *"Delitos informáticos realizados en actuación organizada", Diario La Ley*, número 7743, 2011, pág.

Comunidades Europeas y posteriormente por la Unión Europea numerosas directivas en materia de propiedad intelectual. Puede así destacarse la Directiva 91/250/CEE, del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador, poniendo así de manifiesto la falta de protección de los mismos en determinados Estados Miembros. La Directiva exponía de forma muy acertada que *"el desarrollo de los programas de ordenador exige una considerable inversión de recursos humanos, técnicos y financieros y que dichos programas pueden copiarse con un coste mínimo en relación con el preciso para crearlos de forma independiente"*, y que, *"considerando que los programas de ordenador están desempeñando un papel de creciente importancia en una amplia gama de sectores y que, en consecuencia, cabe considerar la tecnología informática como de capital importancia para el desarrollo industrial de la Comunidad"*. Igualmente destacable es la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos; dicha especial necesidad de protección, se da entre otros, por lo siguientes motivos: *"la fabricación de una base de datos requiere una gran inversión en términos de recursos humanos, técnicos y económicos, y que las bases de datos se pueden copiar o se puede acceder a ellas a un coste muy inferior al necesario para crearlas de forma independiente[…]la extracción y/o reutilización no autorizadas del contenido de una base de datos son actos que pueden tener consecuencias graves desde el punto de vista económico y técnico",* que además *"las bases de datos constituyen un instrumento de gran valor para el desarrollo del mercado comunitario de la información; que este instrumento es de gran utilidad para otras muchas actividades[…] la presente Directiva protege las recopilaciones, también llamadas «compilaciones», de obras, de datos o de otras materias cuya disposición, almacenamiento y acceso se efectúen mediante procedimientos electrónicos, electromagnéticos, electroópticos u otros similares[…]los criterios en virtud de los cuales las bases de datos son susceptibles de la protección de derechos de autor deben limitarse al hecho de que la selección o disposición del contenido de la base de datos constituya una labor de creación intelectual propia del autor; que esta protección se refiere a la estructura de la base de datos".*

Por otro lado, se adopta en el año 1993 la Directiva 93/98/CEE, del Consejo, de 29 de octubre de 1993, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines, y junto con ella, la Ley 27/1995, de 11 de octubre, encargada de la incorporación al derecho español de dicha Directiva en cuanto

mediante la misma se dio una habilitación legislativa al Gobierno de la época para la aprobación de un texto que refundiere las disposiciones legales en materia de propiedad intelectual. Fue así como en el año 1996 se aprobó mediante Real Decreto Legislativo 1/1996, de 12 de abril, el Texto Refundido de la Ley de Propiedad Intelectual, entrando en vigor la misma el 23 de abril de ese mismo año.

Y si bien la citada Ley de Propiedad Intelectual ha sido objeto de numerosas modificaciones, se centrará sin embargo el presente trabajo en el ámbito de protección jurídico penal en materia de propiedad intelectual, no ahondando así, en aras de sintetizar el presente trabajo, en el desarrollo de las citadas reformas y centrándose en la regulación realizada por el Código Penal, y en la evolución normativa sufrida por la misma.

En el ámbito penal, se recogían ya por el Decreto de 23 de diciembre de 1944, por el que se aprueba y promulga el "Código Penal, texto refundido de 1944", según la autorización otorgada por la Ley de 19 de julio de 1944, los delitos contra la propiedad intelectual e industrial dentro del libro II, título XIII, capítulo IV, sección 2ª, *"de las estafas y otros engaños"*, y más concretamente, por el artículo 533 del citado texto, disponiendo en concreto que *"incurrirán en las penas señaladas en el artículo 531 los que cometieren alguna defraudación de la propiedad intelectual o industrial",* texto que fue posteriormente modificado en el año 1963 por el Decreto 691/1963, de 28 de marzo, por el que se aprueba el "Texto revisado de 1963" del Código Penal, libro II, título XIII, capítulo IV *"de las defraudaciones"*, sección 3ª *"de las infracciones del derecho de autor y de la propiedad industrial",* que disponía en concreto en su artículo 534 que, *"el que infringiere intencionadamente los derechos de autor será castigado con las penas de arresto mayor y multa de 10.000 a 100.000 pesetas, independientemente de las sanciones determinadas en las leyes especiales. La misma pena se aplicará a los que de igual manera infringieren los derechos de propiedad industrial. La reincidencia, en ambos casos, se castigará con la pena de prisión menor*". Posteriormente, en el año 1973, se publicó un Texto Refundido por Decreto 3096/1973, de 14 de septiembre, por el que se publica el Código Penal, Texto Refundido conforme a la Ley 44/1971, de 15 de noviembre, por el que no se produjo modificación en materia de *"derechos de autor"*. E igualmente, tras la reforma operada por la Ley Orgánica 8/1983, de 25 de junio, de Reforma Urgente y Parcial del Código Penal, tampoco se produce modificación al respecto.

Posteriormente, tras no sufrir reforma alguna durante las diversas modificaciones sufridas por el Código Penal en los años sucesivos, se produce en esta materia una reforma relevante con la publicación de la Ley Orgánica 6/1987, de 11 de noviembre, por la que se modifica la sección III del capítulo IV, título XIII del libro II del Código Penal, estructurando la sección respectiva a *"las infracciones del derecho de autor y de la propiedad industrial"* en cuatro artículos; así, se recogía por el artículo 534 bis a) del texto mencionado con anterioridad el tipo básico, artículo que refería que *"será castigado con la pena multa de 30.000 a 600.000 pesetas quien intencionadamente reprodujere, plagiare, distribuyere o comunicaré públicamente, en todo o en parte, una obra literaria, artística o científica o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quien intencionalmente importaré, exportaré o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización"*. Por otro lado, el artículo 534 bis b) recogía los supuestos agravados, y en concreto disponía: *"1. Será castigado con la pena de arresto mayor y multa de 50.000 a 1.500.000 pesetas quien realizare cualquiera de las conductas tipificadas en el artículo anterior, concurriendo alguna de las siguientes circunstancias: a) Obrar con ánimo de lucro b) Infringir el derecho de divulgación del autor c) Usurpar la condición de autor sobre una obra o parte de ella o el nombre de un artista en una interpretación o ejecución d) Modificar sustancialmente la Integridad de la obra sin autorización del autor. 2. Se impondrá la pena de prisión menor, multa de 50.000 a 3.000.000 de pesetas e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando, además de obrar con ánimo de lucro concurra alguna de las siguientes circunstancias: a) Que la cantidad o el valor de las copias ilícitas posean especial trascendencia económica B) Que el daño causado revista especial gravedad. En tales supuestos el Juez podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado"*. Mencionar también el artículo 534 bis c), que recogía una fórmula, que como se verá en sucesivos apartados ha perdurado en el tiempo, en concreto en el actual artículo 272.2 del vigente Código Penal, siendo la misma la siguiente: *"en el supuesto de sentencia condenatoria el Juez podrá decretar la publicación de ésta, a costa del infractor, en un periódico oficial",* e igualmente, como sucedía en el anterior caso, se mantiene en cierto modo la fórmula empleada por el artículo 534 ter, refiriendo la

regulación de la responsabilidad civil por el texto de la Ley de Propiedad Intelectual, manteniendo así una gran similitud al vigente artículo 272.1 del Código Penal, pues en concreto disponía que *"la extensión de la responsabilidad civil derivada de los delitos tipificados en los artículos 534 bis a) y 534 bis b) se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios".*

Más adelante se modificaron por la Ley Orgánica 3/1989, de 21 de junio, de actualización del Código Penal, las cuantías de las penas multa recogidas por los artículos 534 bis a), pasando la misma de 30.000 a 600.000 pesetas a 100.000 a 2.000.000 pesetas, por el artículo 534 bis b).1 de 50.000 a 1.500.000 pesetas a 175.000 a 5.000.000 pesetas, y por el artículo 534 bis b. 2 de 50.000 a 3.000.000 de pesetas a 175.000 a 10.000.000 pesetas.

Tras varios proyectos de Código Penal, ve la luz finalmente la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que, en su redacción original, recogía en su artículo 270 que *"será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador";* en su artículo 271 que *"se impondrá la pena de prisión de un año a cuatro años, multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias: a) Que el beneficio obtenido posea especial trascendencia económica. b) Que el daño causado revista especial gravedad. En tales casos, el Juez o Tribunal podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. El cierre temporal no podrá exceder de cinco años";* y en su artículo 272 se

disponía que *"1. La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios. 2. En el supuesto de sentencia condenatoria, el Juez o Tribunal podrá decretar la publicación de ésta, a costa del infractor, en un periódico oficial".*

En el año 2003, se modifica por la Ley Orgánica 15/2003, de 25 de noviembre, el Código Penal, en concreto, se realiza una restructuración del artículo 270, realizando en primer lugar una numeración de los párrafos, si bien la única modificación del contenido del citado artículo fue la inclusión en el segundo apartado, relativo a la exportación o almacenamiento del supuesto de importación intencionada y sin autorización; así, se añade que *"igualmente incurrirán en la misma pena los que importen intencionadamente estos productos sin dicha autorización, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia ; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento".* Por otro lado, se efectúan modificaciones en el artículo 271, realizando en primer lugar una subida de la horquilla punitiva de la pena de multa, pasando de los ocho a veinticuatro meses a una pena de doce a veinticuatro meses. Se mantiene respecto del artículo anteriormente citado intacto el apartado a) y se introduce una modificación respecto del b), quedando el referido apartado como se expone a continuación: *"que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente o a la especial importancia de los perjuicios ocasionados". P*or otro lado, se añaden dos nuevos apartados c) y d), los cuales recogen respectivamente "*que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual"* y *"que se utilice a menores de 18 años para cometer estos delitos";* finalmente, respecto del artículo 271, se suprime el párrafo que disponía que *"en tales casos, el Juez o Tribunal podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. El cierre temporal no podrá exceder de cinco años".*

De nuevo, en el año 2010, se modifica el Código Penal por la Ley Orgánica 5/2010, de 22 de junio; en este sentido, se modifica únicamente el artículo 271, introduciendo en el apartado primero, un segundo párrafo, en el que se disponía que *"no*

obstante, en los casos de distribución al por menor, atendidas las características del culpable y la reducida cuantía del beneficio económico, siempre que no concurra ninguna de las circunstancias del artículo siguiente, el Juez podrá imponer la pena de multa de tres a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo 623.5". Dicha reforma operada por la Ley Orgánica 5/2010, de 22 de junio, se fundamentó, como se expone en el apartado XVII de su preámbulo, en que *"en el ámbito de los delitos relativos a la propiedad intelectual e industrial ha evidenciado una cierta quiebra de la necesaria proporcionalidad de la pena en el caso de conductas consistentes en la venta a pequeña escala de copias fraudulentas de obras amparadas por tales derechos, máxime cuando frecuentemente los autores de este tipo de conductas son personas en situaciones de pobreza, a veces utilizados por organizaciones criminales, que con tales actos aspiran a alcanzar ingresos mínimos de subsistencia".*

Finalmente, en el año 2015 se modifica de nuevo el Código Penal, en concreto por la Ley Orgánica 1/2015, de 30 de marzo. En este sentido, sufre el artículo 270 una severa modificación, pasando a organizarse mediante seis numerarios (en lugar de tres como en su anterior redacción).

Así, si bien el numerario primero mantiene la línea argumental seguida hasta entonces, queda redactado como se expone a continuación: *"será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios"*. Por un lado, se produce una agravación de la pena en atención a la regulación anterior, pasando de una pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses, a una pena de prisión de seis meses a cuatro años, manteniendo en este caso la pena de multa de doce a veinticuatro meses. Por otro lado, se sustituye la expresión *"ánimo de lucro"* por la de *"ánimo de obtener un beneficio económico directo o indirecto",* manteniendo como es obvio el criterio del perjuicio a tercero. Se completa

también la acción típica, dado que, si bien se recogían los supuestos de reproducción, el plagio, la distribución y la comunicación pública, se incluye ahora por el legislador la expresión *"o de cualquier otro modo explote económicamente"*, realizando lo que parece una apertura conceptual que pretende encuadrar conductas futuras que pretendan atentar contra el bien jurídico protegido. Por último, respecto al artículo 271.1 del Código Penal, se mantiene su redacción en lo relativo a la transformación, interpretación o ejecución sin autorización de los titulares de los derechos o sus cesionarios, y se elimina el párrafo 2º relativo a la distribución al por menor (que era castigado como falta, siendo las mismas suprimidas) y que, sin embargo, como se analizará *infra*, parece haber sido recogido en cierto modo por el artículo 270.4 del Código Penal.

Se recoge como novedad por el artículo 270.2 del Código Penal que *"la misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios"*, introduciendo así la tipificación de la facilitación, que se analizará en posteriores epígrafes.

Igualmente novedosa es la redacción del artículo 270.3 del Código Penal, en cuanto dispone que *"en estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual. Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente"*, facultando así a jueces y tribunales para la correspondiente retirada del material objeto de infracción, la interrupción de prestación de servicio de portales web, así como la adopción de las medidas cautelares que estimen

pertinentes, pudiendo incluso llegar a bloquear en casos excepcionales el acceso a tales sitios web.

Como se adelantó, parece querer el legislador mantener cierta proporcionalidad en las penas (como así dejo claro tras la ya mencionada reforma del año 2010) para aquellos casos en los que la conducta revista una menor gravedad. Así, el artículo 270.4 del Código Penal establece que *"en los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años. No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días".*

Respecto del artículo 270.5 del Código Penal, se mantiene la tipificación de supuestos de exportación, almacenamiento e importación de productos sin autorización, pero se añaden supuestos de favorecimiento o facilitación, eliminando o modificando medidas tecnológicas eficaces incorporadas en los productos para impedir o restringir su realización y la facilitación a terceros de acceso, transformación, interpretación o ejecución artística de bienes protegidos eludiendo o facilitando la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo, quedando en concreto la redacción como sigue: *"serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes: a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente. b) Importen intencionadamente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento. c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces*

incorporadas por éstos con la finalidad de impedir o restringir su realización. d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo".

Finalmente, respecto de las modificaciones operadas en el artículo 270, se mantiene prácticamente en el apartado sexto la redacción anterior (que se encontraba recogida por el artículo 270.3 en la redacción del año 2010) por la que se tipifica la fabricación, importación, puesta en circulación y posesión con finalidades comerciales de medios que permitan la facilitación, supresión no autorizada o la neutralización de dispositivos técnicos concebidos para proteger programas de ordenador u otras obras, interpretaciones o ejecuciones. Se realiza una agravación de la pena, pasando la misma de seis meses a dos años y multa de 12 a 24 meses, a una de prisión de seis meses a tres años, quedando la redacción del modo siguiente: *"será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo".*

No son pocas tampoco las modificaciones operadas sobre el artículo 271 del Código Penal, relativo a los supuestos de agravación. Se realiza en primer lugar una agravación de la pena respecto a la de la anterior redacción, pasando de una pena de prisión de uno a cuatro años, multa de 12 a 24 meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, a una pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años. Además, si bien no son ciertamente notorias, se realizan modificaciones en la redacción de los apartados a) y b) completando la redacción ya existente y quedando la misma respecto del apartado a) *"que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica"*,

incluyendo así la formula *"o que se hubiera podido obtener",* y respecto del apartado b), *"que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente, el número de obras, o de la transformación, ejecución o interpretación de las mismas, ilícitamente reproducidas, distribuidas, comunicadas al público o puestas a su disposición, o a la especial importancia de los perjuicios ocasionados",* incluyendo así la formula *"el número de obras, o de la transformación, ejecución o interpretación de las mismas, ilícitamente reproducidas, distribuidas, comunicadas al público o puestas a su disposición",* existiendo así nuevos criterios que permiten entender la concurrencia de una especial gravedad.

Por último, no se realiza de nuevo, como ya ocurrió en el año 2010, ningún tipo de modificación en la redacción del artículo 272 del Código Penal, el cual continua con su redacción original del año 1995.

3. Bien jurídico protegido

No entraña duda alguna, a raíz de la redacción ofrecida por el legislador, la configuración de la propiedad intelectual como un derecho con una doble vertiente, desprendiéndose tal tesis de la propia Ley de Propiedad Intelectual, cuando dispone en su artículo 2 del citado texto que *"la propiedad intelectual está integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley".* Pueden así diferenciarse, por una parte, los derechos personales o morales del autor (que podríamos llamar extrapatrimoniales), recogidos por la propia Ley de Propiedad Intelectual en los artículos 14 a 16 de dicho texto, siendo los mismos irrenunciables e inalienables, como por ejemplo, entre muchos otros, los derechos a decidir si su obra ha de ser divulgada y en qué forma, o exigir el reconocimiento de su condición de autor de la obra, y, por otra parte, derechos patrimoniales, los cuales son definidos por la ley anteriormente citada como derechos de explotación, en concreto, por los artículos 17 y siguientes, exponiendo el artículo 17 que *"corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización".*

Y si bien sería ciertamente interesante la realización de un análisis detallado de la vertiente moral o personal de la propiedad intelectual, ello únicamente extendería de manera innecesaria el presente trabajo, pues se adelanta que será únicamente objeto de protección jurídico-penal la misma de concurrir una afección de la vertiente patrimonial. Así, como bien expone CASTIÑEIRA PALOU, *"la reforma de 1987 supone una toma de posición clara por parte de Legislador en favor de la protección del derecho moral de autor […] pero esta situación no duró mucho, ya que el CP de 1995 modificó el tipo básico de los delitos contra la propiedad intelectual e introdujo el «ánimo de lucro y el perjuicio de tercero» como elementos del tipo. El Código Penal vigente vuelve a colocar en primer término el contenido económico de los derechos de propiedad intelectual, de modo que, si se lesiona sólo el derecho moral de autor, no hay responsabilidad penal. El Legislador ha considerado correctamente que para estos casos era suficiente el Derecho civil"*[225]. Por ende, dado el principio de *ultima ratio* del Derecho penal, de la ubicación sistemática dentro del libro II, título XIII, relativo a los delitos contra el patrimonio y contra el orden socioeconómico, y de la inclusión por el legislador de las fórmulas *"con ánimo de obtener un beneficio económico directo o indirecto"* y *"en perjuicio de tercero"*, puede concluirse, al compás de la doctrina mayoritaria, que la vertiente moral de la propiedad intelectual será únicamente relevante en términos de protección jurídico-penal cuando se produzca junto a la misma una afección de la vertiente patrimonial, quedando en caso contrario relegada la protección de la misma al ámbito civil. En este sentido, TASENDE CALVO dispone que *"la polémica doctrinal sobre el bien jurídico protegido ha quedado zanjada por el Legislador, que claramente ha optado por la protección de los intereses patrimoniales que subyacen bajo los distintos aspectos de la propiedad intelectual"*[226].

Así, por ejemplo, si bien el artículo 270 del Código Penal recoge el supuesto de plagio, y consistiendo el mismo, según la RAE, en la acción de *"copiar en lo sustancial obras ajenas, dándolas como propias",* el cual podría entenderse como una manifestación de los derechos morales del autor mediante la que se protege en un principio, *"la paternidad, integridad, respeto a la esencia y contenido de la obra"*[227]. Sin embargo, se

[225] CASTIÑEIRA PALOU, M.T., *"Bien jurídico protegido e interpretación de los delitos contra la propiedad intelectual"*, en *Derecho Penal del Estado social y democrático de derecho. Libro homenaje a Santiago Mir Puig*, Editorial La Ley, Madrid, 2010, págs.741 y ss.
[226] TASENDE CALVO, J., *"Los delitos contra la propiedad intelectual. Tipicidad y doctrina legal", Actualidad Penal*, número 24, 2003, pág. 615.
[227] MATA Y MARTÍN, R.M., *Delincuencia informática…*, pág. 88.

hace únicamente penalmente relevante en tanto exista aparejado un ánimo de obtener un beneficio económico directo o indirecto, en perjuicio de tercero. En este sentido igualmente se expresa TIRADO ESTRADA en tanto dispone que *"el plagio con trascendencia jurídico-penal, por tanto, deberá ser un plagio con trascendencia productiva económica de cierto alcance e impacto patrimonial, ya que sólo indirectamente, como asociada a la faceta patrimonial, se protege la facultad moral con la que se relaciona"*[228].

Pese al consenso doctrinal existente respecto de la protección penal de la faceta o vertiente patrimonial de la propiedad intelectual, no se da de igual forma tal consenso respecto del concreto bien jurídico protegido por los tipos relativos a la propiedad intelectual. Así, un sector doctrinal entiende la protección de un bien jurídico supraindividual, el orden socioeconómico, y otro la protección de un bien jurídico individual, el patrimonio.

Como se adelantaba, no son pocos los autores que entienden la protección del bien jurídico supraindividual *"orden socioeconómico"*, así, por ejemplo, GONZÁLEZ RUS[229] entendía ello, en el año 1999, debido a la ubicación sistemática de los tipos relativos a la propiedad intelectual, dentro del libro II, título XIII, capitulo XI, correspondientes a "*los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores".* Por otro lado, entendía el citado autor que, dada la potencialidad de las conductas para la incidencia en el mercado, deben excluirse del ámbito de la responsabilidad penal, aquellas conductas producidas en un ámbito estrictamente privado, dado que no gozan de tal potencialidad lesiva. Respecto de la incidencia de las conductas que atentan contra la propiedad intelectual, expone IGLESIAS RIO que *"la propiedad intelectual se proyecta en una dimensión supraindividual, colectiva, socioeconómica, que trata de preservar un correcto funcionamiento del mercado, con referencia a la relevancia constitucional de protección al acceso a la cultura, a los resultados y avances de la investigación e innovación, a la promoción del progreso científico, del ingenio, e*

[228] TIRADO ESTRADA, J.J., "*Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear y el nuevo tipo de facilitación del acceso y localización en internet de contenidos protegidos", Actualidad Civil*, número 6, 2017, pág. 12.
[229] Cfr. GONZÁLEZ RUS, J.J., *"Protección penal de sistemas, elementos, datos, documentos y programas informáticos"*, *Revista Electrónica de Ciencia Penal y Criminología*, número 1, 1999, en http://criminet.ugr.es/recpc/recpc_01-14.html.

instando a que las creaciones reviertan en la comunidad"[230]. Y, por otro lado, respecto de la exclusión de las conductas producidas en el ámbito estrictamente privado, MESTRE DELGADO expone *que "de todas las agresiones que pueden recibir los derechos de propiedad intelectual, el Código Penal selecciona, como delictivas, las más graves […] en efecto, la consideración de los delitos contra la propiedad intelectual como delitos contra el orden socioeconómico exige limitar el ámbito de lo punible a las conductas que lesionen los bienes jurídicos protegidos en esta categoría delincuencial. Por ello, debe estimarse que sólo forman parte del ilícito las conductas de trascendencia económica (remitiendo al ámbito de protección civil aquellas que tan solo lesionen, sin mayor alcance, los derechos morales del autor), y solo en la medida en que repercutan en el ejercicio social de los derechos propios del mismo (quedando al margen de lo punible, y deferidos al ámbito de la responsabilidad civil, en su caso, las acciones que no desplieguen esta trascendencia ante la colectividad)"*[231].

También TIRADO ESTRADA entiende la trascendencia socioeconómica de este tipo de delitos, refiriendo que *"las conductas vulneradoras de derechos de propiedad intelectual, cuya dimensión socioeconómica trasciende lo puramente privado […] ello permite tener la propiedad intelectual como bien jurídico digno de protección también desde la perspectiva del interés general en atención a su considerable trascendencia para la colectividad social, por más que el bien jurídicamente tutelado con carácter inmediato venga constituido por el derecho exclusivo de los legítimos titulares a la explotación económica de la obra o prestación en todas sus modalidades"*[232], y sin embargo, el autor reconoce que, pese a que el bien jurídico tutelado sea el patrimonio en sentido individual, entiende prima la trascendencia para la colectividad de este tipo de conductas; así, expone que *"el fenómeno de la piratería, en el que se constata la instalación de organizaciones y grupos delincuenciales organizados, es percibido como un factor con notable incidencia también en intereses públicos colectivos, en cuanto genera efectos negativos a nivel de entramado industrial, empleos, impuestos, cuotas a la seguridad social"*[233].

---

[230] IGLESIAS RIO, M.A., *El plagio en el marco de los delitos contra la propiedad intelectual", en "La propiedad intelectual en las universidades públicas*, Comares, Granada, 2016, págs. 223 a 253.
[231] MESTRE DELGADO, E., *op.cit.*, pág. 465.
[232] TIRADO ESTRADA, J.J., *"Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear…"*, pág. 2.
[233] TIRADO ESTRADA, J.J., *"Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear…"*, pág. 2.

En este sentido, parece apoyar dichas tesis la redacción del artículo 10 del Convenio de Budapest de 23 de noviembre de 2001, sobre la ciberdelincuencia, en cuanto dispone que *"cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual […] a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial",* recogiendo así la fórmula *"escala comercial",* que parece indicar la protección de dicho orden socioeconómico (demostrando una mala transposición por el legislador nacional), y por otro lado, la Circular 1/2006, sobre delitos contra la propiedad intelectual e industrial, tras la reforma de la Ley Orgánica 15/2003, y la Circular 8/2015, sobre los delitos contra la propiedad intelectual cometidos a través de los servidores de la sociedad de la información, tras la reforma operada por la Ley Orgánica 1/2015, en tanto entienden *"el elemento subjetivo […] exigido por el tipo penal no puede tener una interpretación amplia o extensiva, sino que debe ser interpretado en el sentido estricto de lucro comercial, relegando al ámbito de las infracciones de carácter civil los supuestos de vulneración de derechos, en los que puede estar implícito un propósito de obtención de algún tipo de ventaja o beneficio distinto del comercial".*

Por otro lado, como ya se adelantaba, otros autores valoran la protección por estos delitos de un bien jurídico individual, el patrimonio; así, por ejemplo, MARTÍNEZ-BUJAN PÉREZ[234] entiende una protección del bien jurídico patrimonial en su faceta o naturaleza individual, no siendo encuadrable en la categoría de delitos contra el orden socioeconómico, y en concreto fundamenta ello en *"la discutible decisión del Legislador de 1995 de incluir estos delitos en el capítulo XI debe atribuirse entonces más bien a la finalidad político-criminal perseguida por el Legislador (ratio legis) que no radica privativamente en la tutela del bien jurídico técnicamente tutelado (el interés patrimonial individual del titular de la propiedad intelectual) sino también en la función de incentivo a la creación y en su incidencia mediata en la práctica en el sistema de libre competencia en el marco de nuestra economía de mercado […] con todo, incluso atendiendo a esta perspectiva su parentesco con los restantes delitos del capítulo es bastante lejano y únicamente puede invocarse al respecto el dato de que en el CP anterior los delitos contra los «derechos de autor» se regulaban juntamente con las infracciones de los derecho de*

[234] MARTÍNEZ-BUJAN PÉREZ, C., *Derecho penal económico y de la empresa. Parte especial*, Tirant Lo Blanch, Valencia, 2015, págs. 174 y 175.

propiedad industrial, prosiguiendo la tradición de reunir las llamadas «propiedades especiales»; pero ese proceder sistemático había sido ya unánimemente criticado por la doctrina especializada, puesto que las razones que cabe aducir para incluir los delitos relativos a la propiedad industrial (pese a tutelar asimismo un bien jurídico de naturaleza puramente individual) en el seno del capítulo I no son trasladables a los delitos contra la propiedad intelectual". Por otro lado, RODRÍGUEZ MORO entiende igualmente que *"el Derecho penal tiene la función de elegir una serie de bienes jurídicos que considera de especial protección castigando los ataques más graves que contra ellos se cometan. Estos bienes jurídicos pueden consistir en derechos, en su totalidad, o parcelas, facultades o intereses derivados de esos derechos, y eso es lo que precisamente efectúa en los delitos relativos a la propiedad intelectual, centrando su objeto de tutela en los intereses patrimoniales y expectativas de ganancia derivados de un grupo de los derechos patrimoniales de propiedad intelectual, los derechos de explotación, es decir, esta parcela concreta del patrimonio individual"*[235]. También FARALDO CABANA[236], cuando expone que *"pese a regularse entre los delitos contra el orden socioeconómico, los delitos relativos a la propiedad intelectual no tutelan bienes jurídicos supraindividuales o colectivos de carácter económico, sino un bien jurídico netamente individual: el aspecto patrimonial de la propiedad intelectual, esto es, los derechos de explotación económica"*. De igual forma, DÍAZ Y GARCÍA CONLLEDO expone que *"el bien jurídico posee naturaleza individual, según se derivaría de la redacción de los tipos (que, entre otras cosas, exigen ausencia de consentimiento o autorización del titular del derecho), frente a lo que piensa un sector minoritario de la doctrina, que ve protegidos intereses socioeconómicos supraindividuales […] esta postura puede aducir en su favor algunos argumentos (incluida la ubicación sistemática de los delitos en el Código), pero lo que se lesiona en cada uno de los tipos […] son derechos individuales de los titulares de la propiedad intelectual o industrial. Sin embargo, el que el bien jurídico sea individual no impide reconocer la trascendencia socioeconómica cada vez mayor de estos delitos y que el Legislador la haya tenido en cuenta (desde luego así lo confiesa expresamente en el apartado iii e de la exposición de motivos de la LO 15/2003,*

[235] RODRÍGUEZ MORO, L., *Tutela penal de la propiedad intelectual*, Tirant lo Blanch, Valencia, 2012, págs. 201 y ss.
[236] FARALDO CABANA, P., *"Estrategias legislativas…"*, págs. 10 y siguientes.

a la que más adelante me referiré) a la hora de configurar los tipos penales"[237]. Por otra parte, parece MUÑOZ CONDE acorde a esta tesis, en cuanto refiere que *"el legislador ha dejado, sin embargo, sin resolver cuáles de los delitos contenidos en el Título XIII son reconducibles al ámbito patrimonial y cuáles al orden socioeconómico. Como ya hemos visto antes (supra capítulo XVI), en la propia sistemática legal, a partir de las Disposiciones comunes a los «delitos patrimoniales» contenidas en los arts. 268 y 269, hay base para decir que todos los delitos que se encuentran tipificados en los Capítulos I a IX son «delitos contra el patrimonio»; mientras que los tipificados en los Capítulos XI a XIV serían «delitos contra el orden socioeconómico». Pero tampoco puede mantenerse este criterio de un modo rígido, porque aun en los Capítulos en los que se tipifican delitos patrimoniales principalmente defraudatorios como la estafa, la apropiación indebida o las insolvencias punibles, pueden incluirse hechos con incidencia en intereses socioeconómicos, y en los Capítulos en los que se tipifican delitos contra el orden socioeconómico hay algunos delitos, como los relativos a la propiedad intelectual o a la receptación, que obedecen más a una estructura de carácter patrimonial que socioeconómica"*[238]. También parece cambiar su criterio GONZALEZ RUS (que como ya se analizó *supra,* en el año 1999, defendía una postura de protección del orden socioeconómico por los delitos de propiedad intelectual), entendiendo en el año 2005 que *"en el sentido real de estos delitos, es a mi juicio, eminentemente patrimonial, sin que el art. 270 ofrezca elementos que permitan ver su contenido una orientación a la tutela de intereses generales o una naturaleza predominantemente socioeconómica. En la regulación de los delitos relativos a la propiedad intelectual predomina la perspectiva concreta del creador y la explotación económica de la obra, lo que evidencia que la protección se aborda prescindiendo de dimensiones más generales y con una inspiración claramente patrimonial, alejando la regulación de las pretensiones colectivas que son propias de las otras figuras del Capítulo, como los delitos contra la propiedad industrial, el mercado o los consumidores, en los que resulta dominante la significación socioeconómica"*[239].

[237] DIAZ Y GARCÍA CONLLEDO, M., *"Delitos contra la propiedad intelectual e industrial. Especial atención a la aplicación práctica en España", Derecho Penal y Criminología*, volumen 30, número 88, 2009, pág. 98.
[238] MUÑOZ CONDE, F., *Derecho penal. Parte espe…,* págs. 425 y ss.
[239] GONZALEZ RUS, J.J., *"Delitos contra el patrimonio y contra…"*, pág. 572.

Al hilo de lo anterior, CASTIÑEIRA PALOU[240] parece posicionarse junto a los autores anteriormente mencionados, pues entiende, primero, que, a pesar de la ubicación sistemática de los delitos contra la propiedad intelectual dentro del libro II, título XIII, relativo a los delitos contra el patrimonio y contra el orden socioeconómico , y en concreto, en el capítulo XI, correspondiente a *"los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores"*, junto a delitos que la autora entiende efectivamente atentan contra el orden socioeconómico, no pueden por ello considerarse contra el orden socioeconómico, puesto que, en su opinión, no es suficiente dicho criterio, requiriéndose así de un análisis de las características concretas de los tipos; segundo, que tampoco es argumento suficiente la posibilidad de persecución *ex officio* de los mismos tras la reforma realizada en el Código Penal por la Ley Orgánica 15/2003, de 25 de noviembre (por la que se modificó el artículo 287 del Código Penal, cambiando la redacción de *"para proceder por los delitos previstos en los artículos anteriores del presente capítulo será necesaria denuncia de la persona agraviada o de sus representantes legales"*, aludiendo así al conjunto del capítulo XI, a *"para proceder por los delitos previstos en la sección 3.ª de este capítulo será necesaria denuncia de la persona agraviada o de sus representantes legales"*, subsumiendo así, únicamente la sección correspondiente a los delitos relativos al mercado y a los consumidores), puesto que entiende que delitos como el hurto y la estafa son igualmente perseguibles de oficio y no por ello se desprende una protección del orden socioeconómico por los mismos; tercero, que se posiciona la autora en contra de la teoría expuesta por PUENTE ALBA[241], la cual realiza una interpretación restrictiva de los elementos ánimo de lucro (actualmente sustituido por la exigencia de un ánimo de obtener un beneficio económico directo o indirecto) y de la exigencia de perjuicio, debiendo así considerarse delictivos aquellos comportamientos que puedan comportar pérdidas económicas relevantes para los titulares de los derechos de propiedad intelectual, como se dijo; en contra, CASTIÑEIRA PALOU entiende que *"se trata de una expresión con un amplio arraigo en el Derecho penal, que, con matices, se ha entendido siempre como la intención de obtener un beneficio patrimonial. En segundo lugar, hay un argumento de más peso: cuando el Legislador ha querido exigir algo distinto del ánimo de lucro, lo ha hecho expresamente […] en los delitos contra la propiedad industrial sí que se exige que se actúe «con fines industriales*

[240]CASTIÑEIRA PALOU, M.T., *"op.cit.*, págs. 6 y 7.
[241] PUENTE ALBA, M.L., *"El ánimo de lucro y el perjuicio como elementos de los delitos contra la propiedad intelectual", Revista Penal*, número 21, 2008, págs. 104 y 105.

[…] o comerciales»"; y en cuarto lugar, en relación con lo anterior, entiende que se desprende de la propia redacción de los preceptos que regulan los delitos contra la propiedad intelectual una defensa de un bien jurídico individual, así, sostiene que *"no hay que pasar por alto el tipo cualificado del art. 271, que establece una pena agravada para los casos en que el beneficio obtenido posea especial trascendencia económica o el que los hechos revistan especial gravedad, atendiendo al valor de los objetos producidos o a la especial importancia de los perjuicios ocasionados. Es cierto que podría considerarse que el tipo básico comprende aquellos hechos que tienen trascendencia económica o que son graves y que el tipo cualificado requiere algo más, pero literalmente el tipo básico del art. 270 no lo requiere […] hay que reconocer que con la letra de la ley no es fácil defender esta interpretación. Si se comparan con los delitos contra la propiedad industrial, que siempre han ido parejos a la intelectual, salvadas las diferencias por razón del objeto de protección, la regulación de ambas figuras es idéntica, los tipos cualificados son iguales en ambos casos. Pero en materia de propiedad industrial sí se hace referencia a la necesidad de que se trate de hechos de una cierta entidad y que requieren una organización humana y material, a través del requisito de fines industriales comerciales interpretado como un elemento de carácter objetivo […]cuando el Legislador ha querido establecer este requisito, lo ha hecho de manera expresa".*

CASTIÑEIRA PALOU, como reflexión final, expone una tercera tesis que podríamos denominar como mixta, consistiendo la misma en el reconocimiento de una vertiente dual de los delitos encuadrados en el Título XIII del Código Penal, relativo a los "*delitos contra el patrimonio y contra el orden socioeconómico",* puesto que entiende que quizá hubiere sido correcto por parte del legislador, de pretender el mismo una clara diferenciación entre ambos, la construcción de dos títulos separados, uno para los delitos contra el patrimonio y otro para el orden socioeconómico; sin embargo, entiende la autora que *"el que se regulen en uno puede explicarse por esos delitos que pueden presentar la doble vertiente. Una estafa de gran entidad puede afectar al orden económico y en consecuencia a bienes jurídicos supraindividuales, de la misma forma que un delito contra la propiedad industrial puede afectar sólo al patrimonio individual"*[242]. Además, "*en la mayor parte de los delitos contra el orden socioeconómico en el fondo subyace una protección al patrimonio individual. En efecto el orden socioeconómico también se ve alterado en el supuesto de que se cometa una infracción contra un bien patrimonial*

[242] CASTIÑEIRA PALOU, M.T., *op.cit.*, pág. 7.

individual, o se lesione o ponga en peligro la producción, distribución o el consumo de bienes y servicios. No ocurre lo mismo a la inversa"[243].

Respecto de la discusión doctrinal anteriormente señalada, como bien indica TIRADO ESTRADA, *"en cualquier caso, la cuestión no está clara y tanto puede defenderse tal interpretación como la contraria, puesto que como contrargumento sólido puede subrayarse que el legislador, de haber tenido dicho designio restrictivo, si hubiera querido, hubiera podido definir una limitación semejante con elementos más precisos y terminantes, como por ejemplo exigiendo en el plano subjetivo fines comerciales en el obrar del agente -como explícitamente hace en exclusiva para el tipo del art. 270.6 CP- o la comisión mediante el desarrollo de una actividad de tipo comercial"*[244]. Hecho que se hace más notorio al realizar como se dijo el legislador una incorrecta trasposición del artículo 10 del Convenio de Budapest de 23 de noviembre de 2001, sobre la ciberdelincuencia, en cuanto dispone la necesidad de adopción de medidas para tipificar como delito aquellas infracciones de la propiedad intelectual que *"se cometan deliberadamente, a escala comercial"*.

Por último, baste hacer remisión, en aras de no reiterar innecesariamente, a la tesis expuesta en la sección relativa al daño informático relativa al bien jurídico, respecto de la inexistencia de un bien jurídico supraindividual o colectivo identificable al conjunto de delitos informáticos[245] como pudieren ser la seguridad informática, la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, la intimidad informática, la tecnología de internet, la información o la confianza en el correcto funcionamiento de los sistemas informáticos como objeto de tutela penal también la calidad, pureza e idoneidad de la información contenida en un sistema informático, el software, internet o la confianza en el correcto funcionamiento de los sistemas informáticos, entre otras propuestas dadas por ciertos autores.

[243] *Ídem.*
[244] TIRADO ESTRADA, J.J., *"Los delitos contra la propiedad intelectual tras la reforma del Código Penal de 2015"* en *La propiedad intelectual en la era digital*, Dykinson, Madrid, 2016, págs. 350 y ss.
[245] FARALDO CABANA, P., *"Estrategias legislativas…"*, págs. 1 y 2.

4. Elementos de la punición

4.1 Ejecución

Los delitos contra la propiedad intelectual se configuran como delitos de mera actividad, integrando la realización de la acción típica todo el desvalor del delito[246]. Ello implica que la ejecución del conjunto de actos ejecutivos conllevaría la consumación directa del tipo, no requiriéndose, por ende, de un resultado posterior al comportamiento realizado. A diferencia de los delitos de resultado ya analizados, no es aquí posible la apreciación de la figura de la tentativa acabada, pues, como se expuso, la ejecución de la conducta implicara directamente su consumación; sin embargo, es de perfecta apreciación la tentativa inacabada recogida por el artículo 16 del Código Penal, cuando no se llegue~~n~~ a producir el conjunto de actos ejecutivos requeridos para la realización del tipo.

En cuanto a la posibilidad de apreciación de comisión activa u omisiva, se desprecia la posibilidad de apreciar una omisión pura o propia en virtud del artículo 10 del Código Penal y dada la ausencia de mención expresa por el legislador, si bien la primera de ellas no entraña dudas. Por otro lado, respecto de la comisión por omisión, recoge el artículo 11 del Código Penal que *"los delitos que consistan en la producción de un resultado sólo se entenderán cometidos por omisión cuando la no evitación del mismo, al infringir un especial deber jurídico del autor, equivalga, según el sentido del texto de la ley, a su causación. A tal efecto se equiparará la omisión a la acción: a) Cuando exista una específica obligación legal o contractual de actuar. b) Cuando el omitente haya creado una los delitos que consistan en la producción de un resultado ocasión de riesgo para el bien jurídicamente protegido mediante una acción u omisión precedente"*, y si bien, autores como GÓMEZ TOMILLO entienden la posibilidad de su concurrencia, en concreto, cuando dispone que *"puede llegarse a la conclusión de que, en ocasiones, estamos ante una conducta omisiva, en la medida en que el sujeto si inicialmente pone a disposición del público la obra (acción positiva), posteriormente, se limita a no impedir su diseminación (omisión, cuando permite la diseminación masiva de la obra). En todo caso, no se alteran las conclusiones sobre la relevancia típica de la conducta en la medida en que entiendo que la comisión por omisión debe estimarse*

[246] MESTRE DELGADO, E., *op.cit.*, pág. 473.

punible. Por una parte, desde el punto de vista formal, la injerencia se constituye en fuente del deber de garantía al haber creado el sujeto la situación de riesgo mediante su acción precedente de poner a disposición de cualquiera a través de Internet la obra", al tenor del texto del artículo 11 del Código Penal, al emplear la formula *"los delitos que consistan en la producción de un resultado"*, parece descartarse expresamente por el Código Penal tal posibilidad, pudiendo por ende despreciarse la apreciación de tal figura al ser los delitos contra la propiedad intelectual de mera actividad, lo cual implica, como ya se expuso, que la realización del conjunto de actos ejecutivos conllevaría la consumación directa del tipo, no exigiéndose así de un resultado posterior.

Son delitos eminentemente dolosos, pues no es posible tampoco la apreciación de la comisión imprudente de este tipo de conductas, en virtud del artículo 12 del Código Penal (*"las acciones u omisiones imprudentes solo se castigarán cuando expresamente lo disponga la ley"),* entendiendo así únicamente apreciable la comisión dolosa de los delitos contra la propiedad intelectual. Además, puede ello desprenderse de la terminología empleada por el legislador, pues el mismo emplea expresiones como *"con ánimo de obtener un beneficio económico"*, *"en perjuicio de tercero"* en los artículos 270.1 y 2 del Código Penal o, *"intencionadamente"* en el artículo 270.5.a) y b), e igualmente, el artículo 270.6, al emplear la formula *"en los términos previstos en los dos primeros apartados de este artículo"*, eliminando así la posibilidad de apreciación de dolo eventual, requiriéndose por ende que el sujeto persiga realizar efectivamente el hecho típico[247].

Respecto a los actos preparatorios, no serán penalmente relevantes las conductas relativas a la provocación, conspiración y proposición (como sí ocurría, por ejemplo, en los delitos de estafa informática en aplicación del artículo 269 del Código Penal), puesto que, por previsión de los artículos 17 y 18 del Código Penal, se castigarán solo y exclusivamente en los casos especialmente previstos por la ley, no realizándose tal previsión para los delitos contra la propiedad intelectual.

4.2 Autoría y participación

Son de perfecta aplicación a los delitos contra la propiedad intelectual los artículos 28 y 29 del Código Penal, relativos a la autoría y participación, si bien, cabe destacar que,

[247] Cfr. MESTRE DELGADO, E., *op.cit.*, pág. 472.

en virtud del artículo 270.6 del Código Penal, se considerará autor de un delito contra la propiedad intelectual a quien fabrique, importe, ponga en circulación o posea con una finalidad comercial medios principalmente concebidos, producidos, adaptados, o realizados para la supresión no autorizada o la neutralización de dispositivos técnicos utilizados para proteger programas u obras sujetas a propiedad intelectual (asimilándose a figuras como la de los artículos 248.2.b) o la del artículo 264 ter). Igualmente relevante resulta la mención del artículo 288 del Código Penal, en relación con el artículo 31 bis del mismo texto, en tanto recoge la responsabilidad de las personas jurídicas para el caso de la realización de esta conductas mediante las mismas, exponiéndose las penas concretas en sucesivos apartados.

4.3 Circunstancias

Son de aplicación para los delitos relativos a la propiedad intelectual casi todas las circunstancias atenuantes y agravantes recogidas en el Código Penal; sin embargo, dada la propia redacción del artículo 22.1º del Código Penal, cuando expone que *"hay alevosía cuando el culpable comete cualquiera de los delitos contra las personas"*, se entiende la inaplicabilidad de dicha circunstancia agravante. Por otro lado, pese a que no se desprende como en el caso anterior de forma literal del propio precepto, puede entenderse de igual manera inaplicable la agravación del artículo 20.5º del Código Penal, relativa al ensañamiento, dado que difícilmente se podrá, en un delito contra la propiedad intelectual, aumentar deliberada e inhumanamente el sufrimiento de la víctima.

Respecto de la circunstancia mixta de parentesco del artículo 23 del Código Penal, no será de aplicación (a diferencia del resto de figuras analizadas en otras secciones) como eximente de responsabilidad criminal, pues ello es solo posible para los delitos de los capítulos I a IX del Código Penal, como señala el capítulo X (*"disposiciones comunes a los capítulos anteriores")*, lo que permite descartar su aplicación a los delitos del capítulo XI. Así, el artículo 23 del Código Penal dispone que *"es circunstancia que puede atenuar o agravar la responsabilidad, según la naturaleza, los motivos y los efectos del delito, ser o haber sido el agraviado cónyuge o persona que esté o haya estado ligada de forma estable por análoga relación de afectividad, o ser ascendiente, descendiente o hermano por naturaleza o adopción del ofensor o de su cónyuge o conviviente"*, siendo habitual en la práctica una aplicación de la misma para delitos que no atentan contra la persona

(como serían los delitos contra la propiedad intelectual) de forma atenuante, debiendo sin embargo analizar las circunstancias de cada caso concreto.

4.4 Penalidad

Se contemplan por los artículos 270.1, 270. 2 y 270.5 del Código Penal los tipos básicos, los cuales imponen pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses, previéndose además para los mismos por el artículo 270.3 la posibilidad de retirada de las obras objeto o prestaciones objeto de infracción, e incluso excepcionalmente el bloqueo del acceso a las mismas. Sin embargo, se prevé para la modalidad básica recogida por el artículo 270.6 del Código Penal, pena de prisión de seis meses a tres años.

Por otro lado, se prevén formas atenuadas en el artículo 270.4 del Código Penal para las conductas recogidas por el artículo 271.1, cuando las mismas consistan en una mera distribución o comercialización ambulante, o se realicen de forma meramente ocasional, castigándose con pena de prisión de seis meses a dos años. Además de lo anterior, se prevé un tipo aún más atenuado por el párrafo segundo del precepto antes referenciado, por el que, en atención a las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiere podido obtener, cuando no concurriere ninguna de las circunstancias previstas por el artículo 271 del Código Penal (que como analizaremos más adelante, corresponde a los supuestos agravados), podrá imponerse pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a setenta días.

Respecto a las modalidades o tipos agravados, se recogen por el artículo 271 del Código Penal penas de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando se cometa alguno de los delitos expuestos con anterioridad concurriendo alguna de las cuatro circunstancias previstas.

Por otro lado, para el caso de responsabilidad por estos delitos de personas jurídicas, dispone el artículo 288 del Código Penal, en relación con el artículo 31 bis del mismo texto, que, para, el caso en que se cometan los delitos previstos en los artículos 270, 271, 273, 274, 275, 276, 283, 285 y 286, se impondrá multa del doble al cuádruple del beneficio obtenido, o que se hubiera podido obtener, si el delito cometido por la

persona física tiene prevista una pena de prisión de más de dos años, o multa del doble al triple del beneficio obtenido, favorecido, o que se hubiera podido obtener, en el resto de los casos.

4.5 Responsabilidad civil

En atención a lo dispuesto por el artículo 272.1 del Código Penal, *"la extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios"*, debiendo acudir para ello a lo dispuesto en el libro tercero, título I, de la Ley de Propiedad Intelectual, y más concretamente a los artículos 138 y siguientes, por los que se recogen supuestos de cese de actividad ilícita y de indemnización (que comprenderá el daño emergente y el lucro cesante por la violación del derecho del autor).

Se prevé igualmente por el artículo 288 del Código Penal la publicación de la sentencia en periódicos oficiales y, a instancia del perjudicado, la reproducción total o parcial en cualquier medio informativo a costa del condenado.

5. Elementos del tipo

5.1 Animo de obtención de un beneficio económico directo o indirecto

Tras la entrada en vigor de la Ley Orgánica 1/2015, de 30 de marzo, se modificó el elemento subjetivo del tipo que hasta el momento consistía en la concurrencia de un *"ánimo de lucro"* del sujeto, pasando en la redacción actual a la necesidad de concurrencia de un *"ánimo de obtener un beneficio económico directo o indirecto"*, cambio realizado con la finalidad, como se expresa en el apartado XVII del preámbulo de la citada ley, de *"abarcar conductas en las que no se llega a producir un lucro directo, pero sí un beneficio indirecto"*. En este sentido es ciertamente ilustrativa la Circular de la Fiscalía General del Estado 8/2015, sobre los delitos contra la propiedad intelectual cometidos a través de servicios de la sociedad de la información tras la reforma operada por la Ley Orgánica 1/2015, en tanto la misma expone que *"el nuevo elemento subjetivo, tomado de la legislación civil y administrativa, donde son habituales los conceptos*

similares al beneficio económico, va a permitir que la intención de obtener ingresos, o cualquier otro rendimiento evaluable económicamente y susceptible de obtenerse por motivo o con ocasión de la realización de una conducta típica, colme la exigencia de actuar con el propósito de obtener un beneficio económico directo o indirecto", es decir, se realiza una apertura conceptual del elemento subjetivo del tipo para una mejor tipificación de estas conductas, adaptando el tipo a los medios comisivos actuales y permitiendo así el encuadre de conductas en las que exista un beneficio indirecto, como por ejemplo, los citados por la propia circular referenciada relativos a la inserción de publicidad sujeta a monetización en páginas web mediante *banners*, *pop-ups*, mediante monetización de visitas (como por ejemplo en la plataforma de YouTube), o mediante el ofrecimiento de tarifas *premium* frente al *free access* a cambio de una cantidad dineraria, entre otros.

5.2 En perjuicio de tercero

Como correctamente señalan MUÑOZ CONDE y GARCÍA ARÁN, a modo de introducción del presente apartado recordar que el tipo penal goza de dos vertientes, una objetiva, es decir, el tipo objetivo, en la que se incluyen "*todos aquellos elementos de naturaleza objetiva que caracterizan objetivamente el supuesto de hecho de la norma penal, o tipo penal (el sujeto activo, la conducta, las formas y medios de la acción, el resultado, la relación de causalidad y los criterios para imputar objetivamente el resultado a la conducta, el objeto material, etc.)"*[248], y una vertiente subjetiva o tipo subjetivo, en la que se encuadra "*el contenido de la voluntad que rige la acción (fin, selección de medios y efectos concomitantes)"*[249]. Al hilo de lo anterior, no se encuentra exento de controversia el elemento típico *"perjuicio de tercero",* puesto que existen dos sectores doctrinales, por un lado, el de los autores que entienden dicho elemento del tipo como subjetivo, y por otro lado, los que se posicionan en el entendimiento de su carácter objetivo.

Por un lado, para el caso de entender el *"perjuicio de tercero"* como un elemento subjetivo del tipo, como consecuencia lógica, se estaría exigiendo la concurrencia de un mero ánimo de causación del mismo, es decir, de una reflexión, finalidad o intención

[248] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho penal. Parte general*, Tirant Lo Blanch, Valencia, 2015, pág. 257.
[249] *Ídem.*

interna del autor que dirige su comportamiento a la causación tal perjuicio. Es decir, que tanto el elemento intelectual o cognitivo (el conocimiento de los elementos que caracterizan objetivamente su acción como conducta típica)[250], como el elemento volitivo (entendido como un ánimo del sujeto de realizar la acción o de producir un resultado, es decir, una voluntad incondicionada de realizar algo [típico] que el autor cree que puede realizar)[251], han de dirigirse hacia la causación de un perjuicio. Así, por ejemplo, MESTRE DELGADO dice que *"todos los delitos contra la propiedad intelectual son dolosos, y no admiten la incriminación imprudente. En todos ellos se exigen, además, elementos subjetivos del injusto característicos, ya que, en las conductas tipificadas en el primer y segundo apartados del art. 270, se establece la necesidad de que la acción típica se realice «con ánimo de obtener un beneficio económico directo o indirecto» y, además, «en perjuicio de tercero» expresión que el Legislador, de forma tradicional, utiliza para determinar la existencia , en el autor del hecho, de una especial finalidad subjetiva que guíe su acción"*[252], y TASENDE CALVO expresa: *"la realización de la conducta «en perjuicio de tercero» revela que estamos ante un delito tendencial y de mera actividad o consumación anticipada en el que, si bien no es necesario que se cause un perjuicio efectivo de terceros, sí es preciso que la acción tenga aptitud o capacidad para producirlo, creando un riesgo o peligro real para su patrimonio aunque no llegue a lesionarlo materialmente. Esta exigencia subjetiva, junto con el ánimo de lucro, excluyen el dolo y la tipicidad de la conducta, cuando ésta obedezca exclusivamente a otros fines, como son los educativos o de estudio"*[253].

Por otro lado, diversos autores entienden la formula *"en perjuicio de tercero"* como un elemento de carácter objetivo que requeriría, en sentido estricto, de la concurrencia de un efectivo perjuicio patrimonial, o entendido de forma más laxa, de una capacidad lesiva de la acción para causar un perjuicio o una aptitud o idoneidad de la conducta para ocasionarlo. Así, señala GONZÁLEZ RUS que *"la consideración como elemento subjetivo del injusto, en cambio, excluiría su aplicación en más casos de los deseables, porque lo común en supuestos de esta naturaleza no es tanto que se quiera perjudicar a otro, cuanto obtener un lucro para sí, por lo que exigir en el sujeto que la conducta tenga como una de sus finalidades causar un perjuicio ajeno, añadido al ánimo*

[250] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho penal. Parte gener…",* pág. 260.
[251] *Ibidem*, pág. 261.
[252] MESTRE DELGADO, E., *op.cit.*, pág. 472.
[253] TASENDE CALVO, J., *op.cit.*, pág. 624.

de lucro, determinaría la impunidad de muchos supuestos. Por eso, a mi juicio, el «en perjuicio» debe interpretarse como una condición objetiva de la conducta, que, por las circunstancias en las que se produce, tiene la idoneidad suficiente para perjudicar a los titulares de los derechos de la propiedad intelectual, lo que constituye un elemento del tipo que debe ser comprendido por el dolo del autor. Ello significa, por ejemplo, que no serán típicas, por falta de esa capacidad potencial, las infracciones que se produzcan para mero uso privado por la misma persona que la lleva a cabo"[254]. En el mismo sentido, MATA Y MARTÍN expone que, de entenderse como elemento subjetivo, *"se trataría de una tendencia interna del autor que debe verificarse mediante su conexión con otros datos externos revelados en los hechos. En general se descarta esta naturaleza subjetiva del elemento, especialmente por cuanto ya hemos visto que el Legislador ha provisto el hecho típico de un claro elemento subjetivo como es el ánimo de lucro lo que no haría necesaria la incorporación de otro más, siendo en tal caso el Legislador innecesariamente reiterativo en lo subjetivo. En sentido objetivo, se representa como idoneidad material de la conducta para causar perjuicios a los titulares de los derechos"*, llegando igualmente el autor al entendimiento del elemento como objetivo del tipo. DÍAZ Y GARCÍA CONLLEDO dispone en términos similares que *"interpretar el «en perjuicio» como simple intención de perjudicar ampliaría desmesuradamente el tipo (aunque lo restringiría también en algún sentido), por lo que descarto esta interpretación, pareciéndome preferible la de exigir perjuicio o, quizá mejor, como interpretación intermedia, la de exigir idoneidad objetiva de la conducta para perjudicar"*[255]. En el mismo sentido, CASTIÑEIRA PALAU entiende que *"la interpretación del perjuicio de tercero es más discutida. Si se concibe como un elemento subjetivo, amplía, todavía más, el ámbito del delito. Si se entiende como un elemento objetivo, la consumación requerirá un efectivo perjuicio patrimonial. Los dos elementos se exigen también en el delito de estafa, allí la exigencia de perjuicio se incluye en el tipo objetivo y exige la concurrencia de un perjuicio patrimonial efectivo. Parece que no hay razones para no interpretarlo de la misma forma en los delitos contra la propiedad intelectual*"[256].

[254]GONZÁLEZ RUS, J.J., "*Protección penal de sistemas…",* recurso electrónico: *http://criminet.ugr.es/recpc/recpc_01-14.html* .
[255] DIAZ Y GARCÍA CONLLEDO, M., *op.cit.*, pág. 115.
[256] CASTIÑEIRA PALOU, M.T., *op.cit.*, pags. 4 y 5.

5.3 Modos de acción

5.3.1 Reproducción

Concepto que consistirá, en atención al artículo 18 de la Ley de Propiedad Intelectual, en la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella que permita su comunicación o la obtención de copias, es decir, en la plasmación de la misma en un soporte útil para tal fin; así pueden destacarse, discos, tarjetas y lápices de memoria discos duros, la propia red, entre otros.

5.3.2 Plagio

Según la RAE, consiste plagiar en el *"copiar en lo sustancial obras ajenas, dándolas como propias",* concepto recogido de manera implícita por el artículo 14 de la Ley de Propiedad Intelectual, por el que se dispone que *"corresponden al autor los siguientes derechos irrenunciables e inalienables: 1.º Decidir si su obra ha de ser divulgada y en qué forma. 2.º Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente. 3. º Exigir el reconocimiento de su condición de autor de la obra"*, entendiendo por ende tal plagio como la usurpación, ante la sociedad, de la condición de autor de la obra ajena, ya sea en su totalidad o de forma parcial[257]. Conducta que, por otro lado, y como ya se mencionó, mantendrá relevancia penal en tanto junto con la misma se produzca una afección de la vertiente patrimonial, puesto que el plagio se ubica en la vertiente moral o personal de los derechos de propiedad intelectual.

5.3.3 Distribución

Ha de entenderse, en atención al artículo 19 de la Ley de Propiedad Intelectual, como distribución la puesta a disposición al público del original, o de las copias de la

[257] MESTRE DELGADO, E., *op.cit.*, pág. 466.

obra, en un soporte tangible, mediante su venta, alquiler, préstamo o mediante cualquier otra forma.

5.3.4 Comunicación pública

En atención al artículo 20 de la Ley de Propiedad Intelectual, consistirá comunicación pública en todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas; actualmente, por ejemplo, mediante la subida de los contenidos a la red, donde cualquier usuario puede acceder al contenido.

Así, por ejemplo, puede citarse la STS 920/2016, de 12 de diciembre, relativa al caso *"youkioske.com",* caso de una asociación cuyo principal objeto era la puesta a disposición en la página www.youkioske.com de publicaciones periódicas y libros sin la autorización de los titulares de los derechos de dichas obras para posteriormente poder ser visionadas y leídas a través de Internet desde cualquier dispositivo electrónico-informático, todo ello, sin contraprestación alguna procedente de los usuarios, consiguiendo los acusados y sus colaboradores, a través de la publicidad ubicada en la citada página, elevadas cantidades de dinero.

Igualmente remarcable es la STS 461/2010, de 6 de julio, que, a pesar de dictarse por la sala de lo civil del citado órgano, determina como acto de comunicación pública la retransmisión de señal de televisión por parte de un Ayuntamiento para su aprovechamiento por los vecinos del municipio.

5.3.5 Explotación económica

Fórmula residual empleada por el legislador, que tipifica las conductas relativas a los delitos informáticos mediante un sistema *numerus apertus;* pretende abarcar aquellas conductas no subsumibles mediante otras figuras. Así, se dispone por el apartado XVII del preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, que *"se añade, para reforzar así la protección que se quiere brindar, la de explotar económicamente de cualquier otro modo una obra o prestación protegida"*.

5.3.6 Facilitación del acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual

Conducta que, además de tener una especial relevancia dado el objeto de estudio del trabajo, como apunta el legislador en el artículo 270.2 del Código Penal, no puede limitarse a un mero tratamiento técnico, sino de un proceder activo y no neutral, de aquellos que, en prestación de servicios en la sociedad de la información, faciliten el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual.

Establece así el legislador una específica forma de ejecución (como mera ejemplificación, dada su relevancia, puesto que se prevé un sistema de *numerus apertus*), como es el ofrecimiento de listados ordenados y clasificados de enlaces a obras y contenidos objeto de protección (pese a que los enlaces hubieren sido en un primer momento aportados o facilitados por los propios destinatarios de sus servicios), como señala TIRADO ESTRADA, centrándose dicha precisión realizada por el legislador en *"páginas de enlace que actúan de atractivos escaparates para el público y, mediante «links», posibilitan el acceso o localización de los contenidos protegidos con base en redes ED2K o sistemas de intercambio de archivos P2P (ya sea con canalización de la búsqueda a través de servidores centrales o de modo descentralizado); descargas directas (FTP) de los archivos alojados desde el servidor donde se hallan; o mediante su reproducción, visualización y/o audición online (streaming) sin incorporación al disco duro del ordenador desde el que se actúa, residiendo los contenidos en servidores de gran capacidad o sirviéndose de portales que facilitan el acceso a eventos en tiempo real"*[258]. En este sentido, parece ilustrativa la SAP Madrid 366/2018, de 29 de mayo, en la que un sujeto, a través de 3 cuentas, gestionaba ocho servidores FTP, descrito por la citada resolución como *"un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos"* , alojados en el extranjero, poniendo a disposición de los usuarios de estos servidores y facilitando su descarga directa, películas, obras fonográficas y videojuegos sin autorización de los titulares de los derechos de explotación

[258] TIRADO ESTRADA, J.J., *"Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear…"*, pág. 23.

sobre los mismos, ofreciendo modalidades de conexión a los citados servidores por precios que oscilaban entre los 10 a 45 euros.

Como señala TIRADO ESTRADA[259], habrá de interpretarse el artículo 270.2 del Código Penal en conjunto la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

5.3.7 Distribución, comercialización ambulante o de forma meramente ocasional

Fenómeno conocido habitualmente bajo la denominación de "top manta" por el uso de los sujetos de mantas para cargar y exponer la mercancía; en este sentido, se hace muy ilustrativa la SAP A Coruña 683/2015, de 6 de mayo, en la que un sujeto en el interior de su vehículo se dedicaba a ofrecer a los viandantes en las inmediaciones de un mercadillo CD´s y DVD´s correspondientes a obras audiovisuales con sus correspondientes caratulas y fundas plásticas (que había obtenido mediante su grabación de los soportes originales), siendo las carátulas también copias, reproducidas mediante un sistema de impresión electrónica, todo ello sin la correspondiente autorización de sus titulares o cesionarios de las citadas obras a los que corresponde derechos de propiedad intelectual sobre las mismas.

5.3.8 Exportación, almacenamiento e importación intencional

Entiende la RAE como exportación el *"vender géneros a otro país"*, y almacenar como *"reunir, guardar o registrar en cantidad algo"*, debiendo ello realizarse respecto de elementos sujetos a derechos de propiedad intelectual, de forma intencional, sin la debida autorización y con la finalidad de su posterior reproducción, distribución o comunicación pública, recogiéndose estos por el artículo 270.5.a) del Código Penal.

Y, si bien no suscitan excesiva duda los supuestos de exportación de productos sujetos a derechos de propiedad intelectual, se hace ilustrativa la SAP Sevilla 276/2007, de 10 de mayo, en cuanto recoge respecto de la conducta relativa al almacenamiento intencional con el fin de su reproducción, distribución o comunicación pública, en concreto, *"el hecho de transportar 302 películas y 295 discos compactos puede*

[259] TIRADO ESTRADA, J.J., *"Los delitos contra la propiedad intelectual tras la reforma del Código Penal",* págs. 350 y ss.

calificarse de almacenamiento, conducta ésta que no tiene una definición legal precisa pero para cuya concreción se puede acudir ante todo al significado gramatical del verbo «almacenar» que, según el Diccionario de la Real Academia, significa en una de sus acepciones simplemente «reunir o guardar muchas cosas». No cabe duda que la tenencia de casi 600 soportes copiados constituye un almacenamiento […] máxime si ponemos esta conducta en relación con las demás conductas típicas que se señalaban en el apartado 1 del mismo artículo 270, entre las que se incluye la distribución y que de alguno de los títulos había hasta 19 copias, lo que excluye claramente el uso privado".

Entiende la RAE por importación *"introducir en un país géneros, artículos o costumbres extranjeros",* siendo indiferente, en los términos expuestos por el artículo 270.5.b) del Código Penal, si los productos sujetos a derechos de propiedad intelectual tienen un origen lícito o ilícito en su país de procedencia (con lo que el legislador parece pretender evitar aquellos supuestos realizados al amparo de legislaciones extranjeras más laxas en materia de propiedad intelectual) cuando los mismos estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, añadiendo el legislador respecto de la importación intracomunitaria, que no obstante la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento, recogiéndose en concreto tal comportamiento por el artículo 270.5.b) del Código Penal. En este sentido, y a modo de ejemplificar, puede citarse la SAP Madrid 1256/2007, de 3 de diciembre, en la que se importan desde China, con objeto de su posterior venta a nivel empresarial en España, productos sujetos a derechos de propiedad intelectual, sin factura y habiendo sido confeccionados sin autorización de los correspondientes titulares de los derechos de propiedad intelectual; en concreto, refiere la citada resolución que se estaba *"importando y almacenando obra reproducida sin la autorización de su autor o productor, como son las imágenes o dibujos de Teletabbies, personajes de Walt Disney, Pato Donald, Mickey etc."*.

5.3.9 Favorecimiento o facilitación mediante la eliminación o modificación de medidas tecnológicas

Conducta recogida por el artículo 270.5.c) del Código Penal, consistiendo según la RAE favorecer en *"ayudar o amparar a alguien o apoyar un intento, empresa u*

opinión", y facilitar como *"hacer fácil o posible la ejecución de algo o la consecución de un fin"*, en este caso, mediante la eliminación o modificación no autorizada de medidas tecnológicas eficaces incorporadas en los mismos con la finalidad de impedir o restringir la realización de conductas recogidas por los artículos 270.1 y 2 del Código Penal, realizando el legislador una redacción ciertamente abierta al no especificar el mismo las formas concretas de facilitación o favorecimiento de la eliminación o modificación de medias tecnológicas, entendiendo por ende subsumible cualquier conducta que conlleve tal facilitación o favorecimiento. En este sentido, habrá de acudirse al artículo 6.3 de la Directiva 2001/29/CE, que entiende por medida tecnológica *"toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos por ley o el derecho sui generis previsto en el Capítulo III de la Directiva 96/9/CE"*, siendo las mismas eficaces cuando *"el uso de la obra o prestación protegidas esté controlado por los titulares de los derechos mediante la aplicación de un control de acceso o un procedimiento de protección, por ejemplo, codificación, aleatorización u otra transformación de la obra o prestación o un mecanismo de control del copiado, que logre este objetivo de protección".*

5.3.10 Elusión o facilitación de la elusión de medidas tecnológicas

Conducta recogida por el artículo 270.5.d) del Código Penal, consistiendo el eludir según la RAE, en *"evitar con astucia una dificultad o una obligación"*. Elusión o facilitación de la elusión de medidas tecnológicas eficaces dispuestas a evitar la misma que ha de realizarse con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica o su transformación, interpretación o ejecución artística, fijado en cualquier tipo de soporte o comunicado a través de cualquier medio, y que, en atención a la redacción de estos tipos, ha de darse sin la concurrencia de una eliminación o modificación de las ya citadas medidas tecnológicas, habiendo de subsumirse en tal caso dentro del supuesto expuesto por el artículo 270.5.c) del Código Penal.

5.3.11 Fabricación, importación, puesta en circulación o posesión con una finalidad comercial de cualquier medio para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones

Como ya se ha mencionado en anteriores secciones, el legislador tiende en la actualidad con figuras como las de los artículos 248.2.b), 264 ter y la presente del artículo 270.6 del Código Penal a un adelantamiento de las barreras de protección creando figuras que *"se consuman sin necesidad de lesión, con el simple peligro […] del bien jurídico, suponiendo por tanto un adelantamiento de las barreras de protección a una fase anterior a la lesión"*[260]. Conductas que por otro lado no dejan de constituir meros actos preparatorios, motivándose en concreto la del artículo 270.6 del Código Penal en atención a lo dispuesto por el apartado XVII del preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, en *"la mejora técnica de la tipificación de la fabricación y puesta en circulación de los medios destinados a facilitar la neutralización de las medidas de protección de la propiedad intelectual, o su posesión con finalidad comercial, ajustando la terminología empleada a la más amplia reflejada en la Directiva 2001/29/CE, así como de la regulación de los supuestos agravados",* Directiva 2001/29/CE que en concreto, en su artículo 6.2, expone que *"los Estados miembros establecerán una protección jurídica adecuada frente a la fabricación, importación, distribución, venta, alquiler, publicidad para la venta o el alquiler, o posesión con fines comerciales, de cualquier dispositivo, producto o componente o la prestación de servicios que: a) sea objeto de una promoción, de una publicidad o de una comercialización con la finalidad de eludir la protección, o b) sólo tenga una finalidad o uso comercial limitado al margen de la elusión de la protección, o c) esté principalmente concebido, producido, adaptado o realizado con la finalidad de permitir o facilitar la elusión de la protección"*, protección que por otro lado no se exige sea penal, pudiendo haberse integrado tal previsión únicamente al orden civil[261].

Así, y sin reiterar demasiado en esta cuestión, puesto que ya se analizó en anteriores apartados, *"todos estos preceptos presentan el factor común de haber sido considerados, por parte de la doctrina mayoritaria, como artículos que crean figuras*

[260] LUZÓN PEÑA, D.M., *op.cit.*, pág. 169.
[261] Cfr. MESTRE DELGADO, E., *op.cit.*, pags. 469 y 470.

delictivas eminentemente orientadas a elevar a la categoría de delitos, lo que, en realidad, no dejarían de ser sino meros actos preparatorios de los delitos a los que cada uno de ellos hacen referencia; actos que permanecerían impunes de no ser por su expresa tipificación, ya que ni siquiera podrían ser considerados como supuestos de conspiración, de proposición o de provocación"[262], expresándose MESTRE DELGADO en el mismo sentido, al entender que *"esta última modalidad delictiva, tipificada en el sexto y último apartado del art. 270 del Código, supone también la incriminación -desproporcionada en desvalor y reproche- de meras conductas preparatorias, que por ello no deberían haber sido equiparadas a las conductas de lesión efectiva"*[263]; en este ámbito, tendrá sentido únicamente el citado artículo 270.6 del Código Penal en tanto se realice por el sujeto la conducta de forma exclusiva, puesto que la posterior realización de la conducta descrita por el resto de tipos básicos por el mismo sujeto fabricante, importador, poseedor de estos medios, absorbería la citada conducta en virtud del artículo 8 del Código Penal.

Conducta de fabricación, importación, puesta en circulación o posesión con una finalidad comercial de medios principalmente concebidos, producidos, adaptados o realizados para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que, por otro lado, habrá de interpretarse en atención a la fórmula empleada por el legislador (*"en los términos previstos en los dos primeros apartados de este artículo")*, es decir, siendo punible únicamente la conducta citada en tanto la misma tenga como finalidad o propósito una posterior realización de las conductas recogidas por los artículos 270.1 y 270.2 el Código Penal, por ende, *"debe restringirse la aplicabilidad de esta previsión a los casos en los que las conductas así tipificadas estén preordenadas a la infracción de un concreto derecho de propiedad intelectual"*[264], no siendo punible por ende la conducta no dirigida a tal fin (como por ejemplo la mera investigación).

Son destacables en este sentido resoluciones judiciales como la SAP Zaragoza 137/2012, de 9 de mayo, en la que establecimientos mercantiles primero, manipulaban, vulnerando los sistemas de seguridad de consolas SONY modelo PSP mediante la instalación de chips, permitiendo la ejecución de juegos no originales, y segundo, disponían de consolas ya "pirateadas" para ser posteriormente comercializadas;

[262] GALAN MUÑOZ, A., *"El nuevo delito del artículo 248.2 CP…"*, pág. 2.
[263] MESTRE DELGADO, E., *op.cit.*, pags. 469 y 470.
[264] MESTRE DELGADO, E., *op.cit.*, pags. 469 y 470.

igualmente la SJP Jerez de la Frontera 414/2011 de 20 de octubre, en la que, en establecimiento mercantil, se comercializaban mecanismos como *"chips"* o programas como el conocido *"swap magic"* para el sistema PlayStation 2, cuyo objeto principal consiste en la supresión o neutralización de dispositivos técnicos usados por los fabricantes (en este caso SONY) para la compatibilidad de sus sistemas únicamente con productos o programas oficiales distribuidos por los fabricantes o sus cesionarios, llegando en reiteradas ocasiones el sujeto a realizar la instalación de los citados chips o programas por una contraprestación económica; y finalmente, la SAP A Coruña 464/2016, de 15 de julio, que de forma muy correcta expone (respecto de la intención del legislador con la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo) que *"al hilo de la reforma llevada a cabo por la LO 1/2015 en cuanto establece «medio especialmente concebido, producido, adoptado o realizado», así con esa tipificación, se estima por la doctrina que el Legislador ha querido evitar la posibilidad de que se dicten en los supuestos de conductas relacionadas con la superación de los dispositivos de protección pronunciamientos absolutorios que se venían dictando en la práctica forense, partiendo de que se entendía la expresión específicamente por la que exclusivamente, declarando la atipicidad de las conductas, que mediante la introducción de chips que, efectivamente, eliminan el sistema de bloqueo de la videoconsola, permitiendo que la misma pueda ser utilizada, por tanto para la utilización de juegos no originales, pero también para convertir la videoconsola en una especia de ordenador personal, apto para realizar el manifiesto de tareas lícitas por lo que el uso de estos chips, no tendría la única finalidad de centralizarlos medios técnicos de protección"*.

5.4 Ausencia de autorización de los titulares o cesionarios

El legislador, mediante el empleo de fórmulas como *"sin la autorización de los titulares o cesionarios", "supresión no autorizada", "sin la referida autorización"* en los delitos contra la propiedad intelectual, o por ejemplo, en los delitos contra la propiedad industrial mediante las fórmulas *"sin consentimiento del titular",* eleva el consentimiento a elemento del tipo (entendiendo la similitud de la expresión autorización a la de consentimiento, puesto que entiende la RAE como autorizar el "dar o reconocer a alguien facultad o derecho para hacer algo", y el consentir como "consentir, el permitir algo o condescender en que se haga", entendiendo la posibilidad de concesión de consentimiento o autorización de forma expresa o tácita siempre y cuando la misma se realice de forma

válida), es decir, en palabras de MUÑOZ CONDE Y GARCÍA ARÁN, *"se concede eficacia al consentimiento del titular del bien jurídico protegido como elemento del tipo de injusto del delito en cuestión"*[265], tesis que, por otro lado, parece reforzar la protección de un bien jurídico individual (el patrimonio) por este tipo de delitos[266]. Así, en concreto, funcionan las fórmulas empleadas por el legislador como un elemento objetivo del tipo común al conjunto de tipos básicos que conforman los delitos contra la propiedad intelectual, y por extensión, a los agravados, siendo determinante dicho elemento de la tipicidad de los mismos, puesto que, de concurrir dicha autorización o consentimiento del titular o de los cesionarios de los derechos de propiedad intelectual, las conductas serían irrelevantes en el ámbito penal, e inclusive, en el ámbito civil.

En opinión de DIAZ Y GARCÍA CONLLEDO, funciona la autorización o consentimiento de los titulares o cesionarios de derechos de propiedad intelectual según las circunstancias como causa de justificación o como causa de exclusión de la tipicidad o de atipicidad [267], tesis acorde a la expuesta por MUÑOZ CONDE y GARCÍA ARÁN, en tanto reconocen que el *"consentimiento, que es una causa de exención de pena que opera a veces como causa de exclusión de la tipicidad y a veces como causa de justificación"*[268], y en cierto modo, con la tesis expuesta por LUZÓN PEÑA, que defiende incluso una tesis más amplia, que podría denominarse como de *"tripartición"*, mediante la que entiende el consentimiento *"como causa de atipicidad por ausencia ya de indicio de antijuridicidad, causa de justificación o como causa de exclusión solo de la tipicidad penal según las circunstancias"*.

Como bien señalan MUÑOZ CONDE y GARCÍA ARÁN, *"esta referencia, expresa o tácita, al consentimiento en algunos tipos penales específicos hace que se le considere más como una causa de exclusión de la tipicidad, que como una causa de justificación"*[269], y más concretamente, respecto de los delitos contra la propiedad intelectual, se recoge el consentimiento o autorización de forma expresa, como elemento objetivo del tipo, entendiendo por ende el mismo *strictu sensu* como una causa de

[265] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho penal. Parte general*, Tirant Lo Blanch, Valencia, 2015, pág. 342.
[266] Cfr. FARRALDO CABANA, P., *"Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio", Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 38/2015, 2015, pág. 11.
[267] DIAZ Y GARCÍA CONLLEDO, M., *op.cit.*, págs. 101 y 102.
[268] MUÑOZ CONDE, F., GARCÍA ARÁN, M., *op.cit.*, pág. 344.
[269] *Ibidem*, pág. 343.

exclusión de la tipicidad o causa de atipicidad por ausencia del citado elemento típico; en este sentido, MESTRE DELGADO refiere que *"el Legislador ha configurado el consentimiento de la víctima como causa de atipicidad de la conducta al exigir en el tipo básico que las acciones constitutivas de la infracción se realicen «sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios»".*

Ahora bien, dicha autorización habrá gozar para su apreciación de una serie de características, pudiendo ser la misma verbal o escrita, entendiendo en principio la necesidad de concurrencia de una autorización expresa, puesto que, si bien es cierto que no se descarta por completo la posibilidad de concurrencia de una autorización tácita, pues, por ejemplo, autores como MATA Y MARTÍN no descartan tal posibilidad (en concreto dispone que *"incluso la prestación auténtica de consentimiento sin reunir los requisitos propios de la regulación de derecho privado produce los mismos efectos destipificadores, de manera que el consentimiento tácito o meramente verbal produciría tales consecuencias"*[270]*).* Como bien señala TIRADO ESTRADA, respecto a las características que han de imbuir a la citada autorización, "*necesidad, existencia, procedencia y validez de la autorización así como sujetos de los que han de provenir (a identificar con los posibles sujetos pasivos del delito) son cuestiones que habrán de examinarse a partir de la regulación establecida en la normativa extrapenal jurídico-privada atendiendo particularmente a los límites temporales y materiales a los derechos que la excusen y a las disposiciones que contienen los requisitos para entenderla concurrente y suficiente"*[271].

No olvidar que se habrá de acudir también para la interpretación del citado elemento a la Ley de Propiedad Intelectual, la cual recoge en los artículos 31 y siguientes supuestos en los que no se requiere de autorización alguna del autor; así es el caso de la reproducción provisional, de la copia privada, cuando se reproduzca, distribuya o comunique públicamente con fines de seguridad pública o para el correcto desarrollo de procedimientos administrativos, judiciales o parlamentarios, actos de reproducción, distribución y comunicación pública de obras ya divulgadas que se realicen en beneficio

[270] MATA Y MARTÍN, R.M., *"El tipo básico de los delitos contra la propiedad intelectual en el ámbito digital"*, en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar probar el delito*, Editorial La Ley, Madrid, 2012, pág. 471.
[271] TIRADO ESTRADA, J.J., *"Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear…"*, págs. 16 y 17.

de personas con discapacidad (en las condiciones expuestas por el artículo 31 ter de la Ley de Propiedad Intelectual), citas y reseñas e ilustración con fines educativos o de investigación científica, entre otros.

Conclusiones

Primera.- Es apreciable en la actualidad un alto grado de arraigo y dependencia de la sociedad hacia las nuevas tecnologías e internet, hecho que, si bien no deja de ser positivo pues estos aportan un sinfín de beneficios como la agilización de tareas, la comunicación y transmisión de datos prácticamente instantánea, también tiene sus inconvenientes, dado que las nuevas tecnologías e internet no se encuentran exentas de comportamientos delictivos, los cuales se desarrollan aprovechando las ventajas anteriormente mencionadas.

Segunda.- Si bien la utilización de las nuevas tecnologías e internet, especialmente por las Administraciones públicas puede ser ciertamente beneficiosa, no deja ello de crear cierto riesgo o vulnerabilidad hacia posibles comportamientos ilícitos que las desestabilicen, ocasionando serios perjuicios, debiendo por tanto extremarse la precaución, creando medidas adecuadas de protección ante la delincuencia informática.

Tercera.- Muchos de los comportamientos ilícitos relacionados con la delincuencia informática podrían evitarse educando a la población sobre este tipo de conductas y las posibles medidas de precaución y protección existentes ante las mismas, bien mediante cursos o la introducción de asignaturas o seminarios en los centros educativos y laborales para su asimilación por la población, que en la actualidad es gran desconocedora de los riesgos que entrañan las nuevas tecnologías.

Cuarta.- La discusión doctrinal que rodea al concepto "delito informático" deja entrever en su trasfondo, independientemente de la terminología defendida por cada autor, y a pesar de la falta de consenso, un constante intento de clasificación o agrupación de las conductas ilícitas relacionadas con las nuevas tecnologías basadas en sistemas informáticos e internet, siendo dicha agrupación posible pese a la diversidad de conductas, en atención a sus características comunes, que sobre todo, radican en las propias características de los medios de comisión o ejecución de las mismas.

Quinta.- Por lo general, los países de nuestro entorno mantienen una regulación de los delitos informáticos muy similar a la de España, diseminando a lo largo de sus codificaciones penales el conjunto de conductas relacionadas con la informática e internet.

Sexta.- Si bien ciertas figuras creadas por el legislador en gran parte debidas a la transposición de tratados internacionales y normativa comunitaria, tendentes al adelantamiento de las barreras de protección (artículos 248.2.b), 264 ter, 270.6 del Código Penal, entre otros) adquieren una cierta funcionalidad cuando las conductas recogidas por los mismos se realizan de forma independiente, por otra parte, entorpecen la aplicación o restan funcionalidad a fórmulas clásicas de participación en determinados casos.

Séptima.- Se aprecia una redacción manifiestamente abierta e indefinida en los tipos encargados de regular la delincuencia informática contra el patrimonio al emplear expresiones como *"artificio semejante"*, *"el que por cualquier medio"*, *"cualesquiera otros medios clandestinos",* ello debido quizá a un intento del legislador de evitar supuestos de laguna legal en concordancia con el rápido avance y desarrollo tecnológico, y que, sin embargo, tiene un difícil encaje con principios como el de legalidad o el de seguridad jurídica, pues si bien es previa y escrita, no puede desprenderse clara en su redacción, siendo encuadrables en su redacción un número elevado de conductas

Octava.-Surge el tipo de estafa informática del artículo 248.2 del Código Penal para cubrir o tipificar aquellas conductas que el tipo de estafa tradicional no lograba abarcar o subsumir por la inexistencia de elementos como el engaño bastante o el error, pues las maquinas no pueden ser engañadas ni caer en error, limitándose las mismas a realizarlas instrucciones, comandos, u órdenes introducidas en los mismos.

Novena.- No deben confundirse, primero, las conductas de los artículos 255 y 283 del Código Penal, pues protegen bienes jurídicos diferentes pese a las manifiestas similitudes que presentan en un principio, y segundo, las conductas de los artículos 255 y 256 del Código Penal entre sí, pues si bien los equipos de telecomunicación harán uso de redes de suministro (red eléctrica o de telecomunicaciones), lo que caracteriza la conducta es el uso perjudicial y no autorizado del equipo terminal de telecomunicaciones.

Decima.-No debe pensarse únicamente respecto de los delitos de daños informáticos en la repercusión a nivel individuo (borrado de documentos, programas, entre otras conductas) sino también a nivel de seguridad de infraestructuras públicas o privadas. Además, ha de entenderse por lo general, un concepto amplio de sistema informático, es decir, concibiendo la posibilidad de subsunción de daños al hardware, cuando con los mismos, se dañe al software o se interrumpa u obstaculice el funcionamiento normal del sistema.

Undécima.- Convendría, en materia de propiedad intelectual, pues es la discusión doctrinal relativa al bien jurídico protegido ciertamente interesante, la realización de una modificación del tipo que establezca una necesidad de realización de estas conductas a escala comercial (como recoge el mal transpuesto por el legislador nacional, artículo 10 del Convenio de Budapest de 23 de noviembre de 2001, sobre la ciberdelincuencia) u otras figuras análogas, como así se hace para la propiedad industrial al exigirse la necesidad de concurrencia de fines industriales o comerciales en la realización de la conducta, de los que se desprende una clara protección del orden socioeconómico.

Duodécima.- Se observa, con el paso del tiempo, un cierto refinamiento de las formulas específicas de comisión en los delitos informáticos, actualizando o buscando los delincuentes al albur de los nuevos avances tecnológicos nuevas formas más depuradas y menos arriesgadas.

Bibliografía

AMADEO GADEA, S., *Código Penal. Doctrina jurisprudencial*, Factum Libri Ediciones, 2015.

ANDRÉS DOMÍNGUEZ, A., *"Los daños informáticos en la Unión Europea", Diario La Ley,* tomo 1, 1999.

ANTON ONECA, J., *"Las estafas y otros engaños, en el Código penal y la jurisprudencia"*, *Nueva Enciclopedia Jurídica*, tomo IX, 1957.

AZCONA ALBARRÁN, C.D., *Tarjetas de pago y derecho penal. Un modelo interpretativo del art. 248.2.c) CP*, Atelier, Barcelona, 2012.

BAJO FERNANDEZ, M., *Los delitos de estafa en el Código Penal*, Editorial Universitaria Ramón Areces, Madrid, 2004.

BARRANCO SAIZ, J., *"Sociedad de la Información"*, *Telos: Cuadernos de comunicación e innovación*, número 69, 2006.

BENITEZ ORTÚZAR, I.F., *"Informática y delito. Aspectos penales relacionados con las nuevas tecnologías"* en *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, Dykinson, Madrid, 2009.

BOLEA BARDÓN, C., ROBLES PLANAS, R., *"La utilización de tarjetas ajenas en cajeros automáticos: ¿Robo, hurto o estafa?"*, *Diario La Ley*, tomo 4, 2011.

CABEDO VILLAMÓN, F., ORTIZ NAVARRO, J.F., AGUADO LÓPEZ, S., *"Conductas típicas y prueba electrónica en los fraudes electrónicos"* en *Fraude electrónico. Panorama actual y medios jurídicos para combatirlo*, Civitas, Navarra, 2013.

CALLE RODRÍGUEZ, M.V., *"El delito de estafa informática"*, *La Ley Penal*, número 37, 2007.

CASTIÑEIRA PALOU, M.T., *"Bien jurídico protegido e interpretación de los delitos contra la propiedad intelectual"*, en *Derecho Penal del Estado social y democrático de derecho. Libro homenaje a Santiago Mir Puig*, Editorial La Ley, Madrid, 2010.

CHOCLÁN MONTALVO, J.A., *"Engaño bastante y deberes de autoprotección"*, *Actualidad Jurídica Aranzadi*, número 398, 1999.

CHOCLAN MONTALVO, J.A., *El delito de estafa*, Bosch, Barcelona, 2000.

CHOCLÁN MONTALVO, J.A, *"Fraude informático y estafa por computación"* en *Internet y derecho penal*, Consejo General del Poder Judicial, Madrid, 2001.

CONDE-PUMPIDO FERREIRO, C., *Estafas*, Tirant lo Blanch, Valencia, 1997.

CORCOY BIDASOLO, M., *"Protección penal del sabotaje informático. Especial consideración de los delitos de daños"*, *Diario La Ley*, 1990.

DE LA CUESTA ARZAMENDI, J.L., PÉREZ MACHIO, A.I., SAN JUAN GUILLEN, C., *"Aproximaciones criminológicas a la realidad de los ciberdelitos"* en *Derecho penal informático*, Civitas, Navarra, 2010.

DE LA MATA BARRANCO, N.J, HERNANDEZ DIAZ, L., *"Los delitos vinculados a la informática en el derecho penal español"* en *Derecho penal informático*, Civitas, Navarra, 2010.

DIAZ Y GARCÍA CONLLEDO, M., "*Delitos contra la propiedad intelectual e industrial. Especial atención a la aplicación práctica en España", Derecho Penal y Criminología*, volumen 30, número 88, 2009.

FARALDO CABANA, P., *"Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática", Eguzkilore*, número 21, 2007.

FARALDO CABANA, P., *"Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación"* en *Un derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz*, Tirant lo Blanch, Valencia, 2011.

FARALDO CABANA, P., *"Los delitos contra el patrimonio tras la reforma de 2010"*, *La Ley Penal*, número 81, 2011.

FARALDO CABANA, P., *"Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio", Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 38/2015, 2015

FARALDO CABANA, P., *"Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio", Revista Aranzadi de Derecho y Nuevas Tecnologías*, número 42/2016, 2016.

FAYOS GARDÓ, A., *"La propiedad intelectual tras la ley 21/2014"*, *Editorial La Ley*, Actualidad Civil, 2015.

FERNÁNDEZ PALMA, R., MORALES GARCÍA, O., *"El delito de daños informáticos y el caso Hispahack"*, *Diario La Ley*, tomo 1, 2000.

FERNANDEZ TERUELO, J.G., *"Respuesta penal frente a fraudes cometidos en internet: Estafa, Estafa informática, y los nudos en la red"*, *Revista de Derecho Penal y Criminología*, número 19, 2007.

FERNANDEZ TERUELO, J.G., *Cibercrimen los delitos cometidos a través de internet*, Constitutio Criminalis Carolina (CCC), Madrid, 2007.

GALAN MUÑOZ, A., *"El nuevo delito del artículo 248.2 CP ¿Un adelantamiento desmedido de las barreras de protección penal del patrimonio?", Diario La Ley,* número 6037, 2004.

GALAN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P*, Tirant lo Blanch, Valencia, 2005.

GALICKI, A., *"Computer Crime", The American criminal law review*, volumen 51, número 4, 2014.

GARCÍA GARCÍA-CERVIGON, J., *"Daños informáticos. Consideraciones penales y criminológicas", Actualidad Jurídica Aranzadi*, 2003, número 588.

GARCIA VALDES, C., MESTRE DELGADO, E., FIGUEROA NAVARRO, C., *Lecciones de derecho penal parte especial*, Edisofer, Madrid, 2015.

GOMEZ INIESTA, D., *"Estafa y blanqueo de dinero a través de internet", La Ley Penal,* número 105, 2013.

GONZÁLEZ CUSSAC, J.L., *et alii*, *Derecho Penal Parte Especial*, Tirant lo Blanch, Valencia, 2016.

GONZÁLEZ HURTADO, J.A., *"Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información"*, *La Ley Penal*, número 107, 2014.

GONZÁLEZ RUS, J.J., *"Protección penal de sistemas, elementos, datos, documentos y programas informáticos"*, *Revista Electrónica de Ciencia Penal y Criminología*, número 1, 1999, en http://criminet.ugr.es/recpc/recpc_01-14.html.

GONZÁLEZ RUS, J.J., *"Delitos contra el patrimonio y contra el orden socioeconómico (VI Apropiación Indebida. Defraudaciones de Fluido Eléctrico y análogas"*, en *Derecho Penal Español: Parte Especial*, Dykinson, Madrid, 2005.

GONZÁLEZ RUS, J.J, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes" en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Comares, Granada, 2006.

GUTIÉRREZ FRANCÉS, M.L., *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991.

HERNÁNDEZ DÍAZ, L., *"El delito informático", Eguzkilore*, número 23, 2009.

IGLESIAS RIO, M.A., *"El plagio en el marco de los delitos contra la propiedad intelectual"*, en *La propiedad intelectual en las universidades públicas*, Comares, Granada, 2016.

JAÉN VALLEJO, M., PERRINO PÉREZ, A.L., *La reforma penal de 2015 análisis de las principales reformas introducidas en el Código Penal por las Leyes Orgánicas 1 y 2/2015 de 30 de marzo*, Dykinson, Madrid, 2015.

JAVATO MARTÍN, A.M., *"Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjeta y otros instrumentos de pago. Recensión del libro de Ricardo M. Mata y Martín*", *Revista Electrónica de Ciencia Penal y Criminología*, número 10, 2008.

LUZÓN CUESTA, J.M., *Compendio de Derecho Penal Parte Especial*, Dykinson, Madrid, 2015.

LUZÓN PEÑA, D.M., *Lecciones de Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 2012.

MANZANARES SAMANIEGO, J.L., *Comentarios al Código Penal. Tras las leyes orgánicas 1/2015, de 30 de marzo, y 2/2015, de 30 de marzo*, Editorial La Ley, Madrid, 2016, recurso electrónico La Ley 3219/2016.

MARCO MOLINA, J., *"Bases históricas y filosóficas y precedentes legislativos del Derecho de autor", Anuario de Derecho Civil,* Volumen 47, número 1, 1994.

MARTÍNEZ-BUJAN PÉREZ, C., *Derecho penal económico y de la empresa. Parte especial*, Tirant Lo Blanch, Valencia, 2015.

MATA Y MARTÍN, R.M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001.

MATA Y MARTÍN, R.M*., "El tipo básico de los delitos contra la propiedad intelectual en el ámbito digital"*, en *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar probar el delito*, Editorial La Ley, Madrid, 2012.

MATUS ACUÑA, J.P., *"Los criterios de distinción entre el concurso de leyes y las restantes figuras concursales en el código penal español de 1995", Anuario de derecho penal y ciencias penales*, tomo 58, 2005.

MAYER LUX, L., *"El bien jurídico protegido en los delitos informáticos", Revista Chilena de Derecho*, volumen 44, número 1, 2017.

MESTRE DELGADO, E., *"Delitos contra el patrimonio y contra el orden socioeconómico"* en LAMARCA (Coord.)., *Delitos. La parte especial del Derecho Penal*, Colex, Madrid, 2015.

MIRÓ LLINARES, F., *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons Ediciones Jurídicas y Sociales, Madrid, 2012.

MIRÓ LLINARES, F., *"La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio"*, *Revista Española de Investigación Criminológica*, número 11, 2013.

MIRÓ LLINARES, F., *"Cibercrimen y vida diaria en el mundo 2.0" en Crimen, oportunidad y vida diaria: libro homenaje al Profesor Dr. Marcus Felson*, Dykinson, Madrid, 2015.

MUÑOZ CONDE, F., GARCÍA ARÁN, M., *Derecho Penal. Parte General*, Tirant lo Blanch, Valencia, 2010.

MUÑOZ CONDE, F., *Derecho penal. Parte especial*, Tirant lo Blanch, México D.F., 2014.

MUÑOZ CONDE, F., *Derecho penal. Parte especial*, Tirant lo Blanch, Valencia, 2017.

OXMAN, N., *"Estafas informáticas a través de internet: acerca de la imputación penal del «phishing» y del «pharming»"*, *Revista de derecho*, número 41.

PÉREZ MACHIO, A.I, *"Consideraciones de derecho comparado: la proyección de la normativa internacional en el tratamiento penal de la delincuencia informática"* en *Derecho penal informático*, Civitas, Navarra, 2010.

POLAINO NAVARRETE, M., *et alii*, *Lecciones de Derecho Penal Parte Especial Tomo II*, Tecnos, Madrid, 2011.

PUENTE ALBA, M.L., "*El ánimo de lucro y el perjuicio como elementos de los delitos contra la propiedad intelectual", Revista Penal*, número 21, 2008.

QUERALT JIMÉNEZ, J.J., *Derecho Penal Español Parte Especial*, Tirant lo Blanch, Valencia, 2015.

QUIGLEY, M., *Encyclopedia of information ethics and security,* Information Science Reference, Hershey, 2008.

RAYÓN BALLESTEROS, M.C., GÓMEZ HERNÁNDEZ, J.A., *"Cibercrimen: particularidades en su investigación y enjuiciamiento", Anuario Jurídico y Económico Escurialense*, Número XLVII, 2014.

REY HUIDOBRO, L.F, *"La estafa informática: relevancia penal del phising y el pharming", La Ley Penal*, número 101, 2013.

RODRÍGUEZ MORO, L., *Tutela penal de la propiedad intelectual*, Tirant lo Blanch, Valencia, 2012.

ROMEO CASABONA, C.M., *"De los delitos informáticos al cibercrimen", en Universitas vitae: homenaje a Ruperto Núñez Barbero*, Editoriales Universidad de Salamanca, Salamanca, 2007.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002.

SANCHEZ BERNAL, J., *"El bien jurídico protegido en el delito de estafa informática"*, *Cuadernos del Tomás*, número 1, 2009.

SERRANO GÓMEZ, A., SERRANO MAÍLLO, A., *Derecho Penal Parte Especial*, Dykinson, Madrid, 2009.

SUAREZ-MIRA RODRIGUEZ, C., JUDEL PRIETO, A., PIÑOL RODRIGUEZ, J.R., *Manual de derecho penal, tomo II (parte especial)*, Civitas, Navarra, 2011.

TASENDE CALVO, J., *"Los delitos contra la propiedad intelectual. Tipicidad y doctrina legal", Actualidad Penal*, número 24, 2003.

TELLEZ VALDES, J., *Derecho informático*, McGraw-Hill, México, 2008.

TIRADO ESTRADA, J.J., *"Los delitos contra la propiedad intelectual tras la reforma del Código Penal de 2015"* en *La propiedad intelectual en la era digital*, Dykinson, Madrid, 2016.

TIRADO ESTRADA, J.J., *"Los delitos relativos a la propiedad intelectual en la era digital. Especial referencia al tipo base nuclear y el nuevo tipo de facilitación del acceso y localización en internet de contenidos protegidos", Actualidad Civil*, número 6, 2017.

VELASCO NÚÑEZ, E., *"Delitos informáticos realizados en actuación organizada*", *Diario La Ley*, número 7743, 2011.

WILLIAMS SHARON, A., "*The Criminal Law Amendment Act 1985: Implications for International Criminal Law"*, *Canadian Yearbook of International Law*, número 23, 1985.

Anexo de jurisprudencia consultada

Tribunal Supremo

-Sentencia del Tribunal Supremo (Sala de lo Penal) de 19 de abril de 1991.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 722/1999, de 6 de mayo.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 561/2001, de 3 de abril.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 2175/2001, de 20 de noviembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 187/2002, de 8 de febrero.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 993/2002, de 27 de mayo.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 1232/2002, de 2 de julio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 948/2002, de 8 de julio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 1476/2004, de 21 de diciembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 185/2006, de 24 de febrero.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 692/2006, de 26 de junio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 369/2007, de 9 de mayo.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 533/2007, de 12 de junio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 1036/2007, de 12 de diciembre

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 860/2008, de 17 de diciembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 476/2009, de 7 de mayo.

-Sentencia del Tribunal Supremo (Sala de lo Civil) núm. 461/2010, de 6 de julio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 987/2012, de 3 de diciembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 621/2014, de 23 de septiembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 832/2014, de 12 de diciembre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 135/2015, de 17 de febrero.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 539/2015, de 1 de octubre.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 377/2016, de 3 de mayo.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 614/2016, de 8 de julio.

-Sentencia del Tribunal Supremo (Sala de lo Penal) núm. 920/2016, de 12 de diciembre.

Audiencias Provinciales

-Sentencia de la Audiencia Provincial de Illes Balears (Sección 2ª) núm. 16/2006 de 18 de enero.

-Sentencia de la Audiencia Provincial de Sevilla (Sección 1ª) núm. 276/2007 de 10 de mayo.

-Sentencia de la Audiencia Provincial de Madrid (Sección 17ª) núm. 1256/2007 de 3 de diciembre.

-Sentencia de la Audiencia Provincial de Ávila (Sección 1ª) núm. 186/2010 de 30 de noviembre.

-Sentencia de la Audiencia Provincial de Zaragoza (número 5) núm. 137/2012 de 9 de mayo.

-Sentencia de la Audiencia Provincial de Valladolid (Sección 4ª) núm. 394/2014 de 22 de septiembre.

-Sentencia de la Audiencia Provincial de Alicante (Sección 2ª) núm. 565/2014 de 31 de octubre.

-Sentencia de la Audiencia Provincial de A Coruña (Sección 6ª) núm. 683/2015 de 6 de mayo.

-Sentencia de la Audiencia Provincial de A Coruña (Sección 2ª) núm. 464/2016 de 15 de julio.

-Sentencia de la Audiencia Provincial de Madrid (Sección 7ª) núm. 366/2018 de 29 de mayo.

Juzgados de lo Penal

-Sentencia del Juzgado de lo Penal de Jerez de la Frontera (Número 1) núm. 414/2011 de 20 de octubre.